Umar Media

انٹرنیٹ استعمال کرنے والوں کے لیے حفاظتی اقدامات

اس کتاب میں آپ کو سکھایا جائے گا کہ کیسے کمپیوٹر، موبائل یا آئی فون پر انٹرنیٹ استعمال کرتے وقت، چند آسان سے سافٹ ویئرز اور احتیاطی سیٹنگز کی مدد سے دشمن کی نظر میں آنے سے اپنے آپ کو محفوظ بنایا جاسکتا ہے۔

تالیف

ابو تراب

https://www.besafer.wordpress.com

صفحہ	فہرستِ مضامین
۴	پیش لفظ
	سیکشن اول۔۔۔۔موبائل سیکیورٹی
۸	اینڈرائیڈ موبائل سیکیورٹی
۸	آئی پی ایڈریس چھپانے اور ڈیٹا انکرپٹ کرنے کیلئے ایف سیکیور فریڈوم کا استعمال
۱۱	براوزر میں لوکیشن ٹریس والے آپشن کو ختم کرنا
۱۲	براوزر کے دیگر احتیاط
۱۳	Web RTC کا مسئلہ
۱۵	لوکیشن یا دوسرے اہم معلومات کے Permissions کو ختم یا محدود کرنا
۱۹	موبائل کو روٹ/Root کرنا
۲۳	روٹ کرنے کے بعد کی چیزیں
۲۷	BBM چلانے اور فرینڈ ایڈ کرنے کا طریقہ
۲۹	فیس بک پر انکرپٹڈ میسیج بھیجنے کا طریقہ
۳۲	اُربوٹ / Orbot استعمال کرنے کا طریقہ
۳۵	ٹیلی گرام میسینجر/Telegram کا استعمال
۳۶	روٹ والے موبائل میں IMEI نمبر تبدیل کرنے طریقہ
۳۸	موبائل میں مزید کچھ احتیاطیں۔۔۔ اینٹی وائرس۔۔۔ فائر وال
۴۰	فیس بک اور ٹیلی گرام کے اکاونٹ ویریفکیشن کیلئے نمبر حاصل کرنے کا طریقہ
۴۳	iOS (یعنی آئی فون اور آئی پیڈ) کی سیکیورٹی
۴۳	سیٹنگز میں ایپ پرمیشن اور دیگر تبدیلیاں
۴۳	لوکیشن کو بند کرنا
۴۴	مائکروفون اور دیگر چیزوں کی پرمیشن کو محدود کرنا
۴۴	ایڈز /اشتہارات کو محدود کرنا
۴۴	iCloud کو بند کرنا:
۴۵	آٹومیٹک اپڈیٹس کو On کرنا
۴۵	پاسورڈ سیٹ کرنا
۴۶	براوزر کے سیٹنگز اور براوزر کا انتخاب
۵۰	پراکسی یعنی آئی پی ایڈریس تبدیل کرنے کیلئے سافٹوئیر کا استعمال
۵۰	ایف سیکیور فریڈوم
۵۱	آواسٹ سیکیور لائن

	سیکشن دوم۔۔۔۔۔کمپیوٹر سیکیورٹی
۵۴	ونڈوز کی سیکیورٹی
۵۴	Windows 8 یا اس سے اوپر والوں میں لوکیشن وغیرہ کو بند کرنا
۵۶	Windows 7 میں ان سیٹنگز کا طریقہ
۵۷	براوزر کے سیٹنگز اور براوزر کا انتخاب
۵۷	TORکا استعمال
۶۰	دیگر براوزرزکا انتخاب اور ان کے سیٹنگزمیں تبدیلی
۶۰	فائر فوکس /Firefox
۶۳	Google Chrome
۶۴	Opera
۶۵	پراکسی (آئی پی ایڈریس تبدیل کرنے) کیلئے F Secure Freedome کا استعمال
۶۷	Antivirus
۶۸	فائر وال/Firewall
۷۰	مزید خفیہ رہنے اور انٹرنیٹ کی مکمل ٹریفک کو انکرپٹ اورٹور کے ذریعے چلانے کیلئے TAILS کا استعمال
۷۳	دیگرچنداہم احتیاطی تدابیر
	سیکشن سوم۔۔۔۔۔ہیکنگ اورہیکنگ سے بچنے کیلئےاحتیاطی تدابیر
۷۴	۱۔فیشنگ
۷۵	اس سے بچنے کا طریقہ
۷۶	۲۔RATs (remote administrative tools)
۷۶	ریٹس سے بچنے کا طریقہ
۷۸	USB، CDs، یا دیگر میموری کارڈ وغیرہ کے آٹو پلے کو بند کرنے کا طریقہ
۸۱	۳۔کی لوگرز/Keyloggers
۸۱	ونڈوز ۱۰ میں پہلے سے انسٹال شدہ کی لاگر کو نکالنے کا طریقہ
۸۳	۴۔ایکس ایس ایس ایکسپلائیٹیشن/XSS Exploitation یا کراس سائٹ اسکرپٹنگ/Cross-site Scripting
۸۳	اس سے بچنے کا طریقہ
۸۳	فیس بک پہ XSS و دیگر ہیکنگ سے بچانے کا طریقہ
۸۶	۵۔مین-اِن-مڈل/ Man-In-Middle
۸۶	۶۔بروٹ فورس/Brute Force
۸۷	بروٹ فورس سے بچنے کیلئےاحتیاطی تدابیر

بسم اللہ الرحمٰن الرحیم

پیشِ لفظ

جس طرح پچھلے زمانوں میں جنگ میں اپنی حفاظت کیلئے زرہیں پہنتے اور ڈھال لیتے اور وہ جنگ کی تیاری کا ایک حصہ تھے بعینہ اسی طرح اس ٹیکنالوجی کے دور میں ایسے احتیاطی تدابیر بھی جنگ کا حصہ ہیں جن کو اختیار نہ کرنے سے دشمن کے حملے کی زد میں آسکتے ہیں، اس لئے تمام مسلمانوں کو چاہئے کہ وہ ان ضروری احتیاطی تدابیر پہ عمل کریں تاکہ کفار و مرتدین کے حملوں سے بچ سکیں۔

ٹیکنالوجی کے اِن شعبوں میں ایک شعبہ انٹرنیٹ کا ہے، جس کے ذریعے مجاہدین ابلاغ کا کام بھی کر رہے ہیں اور اس کے ذریعے دیگر جہادی کام بھی ہو رہے ہیں، مثلاً کسی جہادی کاروائی کو پائے تکمیل تک پہنچانے کیلئے معلوماتی کام، آپس میں رابطہ، دیگر حرب کے علوم کو سیکھنا وغیرہ، یہ تمام کام انٹرنیٹ کے ذریعے ہی ہو رہے ہیں۔
انٹرنیٹ پہ بھی کفار اور مرتدین کے لوگ بیٹھے ہوئے ہیں جن کا کام صرف اُن لوگوں کا پتا لگانا ہے اور معلومات حاصل کرنا ہے جو انٹرنیٹ پہ جہاد کو فروغ دے رہے ہیں اور جو مجاہدین کی حمایت کر رہے ہیں، پھر اُنہی معلومات کے ذریعے سے اُن کے خلاف موثر اقدام کرنا ہے۔
تو اس لئے یہ ضروری سمجھا کہ مجاہدین اور اُن کے انصار کو انٹرنیٹ پہ احتیاطی تدابیر کے حوالے سے بتایا جائے، اسی کی ایک کاوش آپ کے سامنے ہے۔

یہ احتیاطی تدابیر اس لئے بتائی جارہی ہیں تاکہ جو لوگ جہاد سے اور مجاہدین سے محبت رکھنے والے ہیں وہ ایجنسی والوں کی خبیث نظر سے محفوظ رہیں، کیونکہ یہی جہاد سے محبت رکھنے والے اس امت کا سرمایہ ہیں اور آگے جاکر انہی کو بڑے کام سرانجام دینے ہونگے تو کیوں ابھی سے احتیاط شروع نہ کریں، ابھی سے اگر احتیاط نہیں کرینگے تو آپ ان ایجنسیوں کی نظر میں ہونگے اور آگے جاکر اگر آپ کوئی کام کرنا چاہیں بھی تو نہیں کر سکیں گے، ہمارا کام تو صرف بات پہنچانا ہے باقی آپ کی مرضی ہے کہ آج سے احتیاط شروع کرنی ہے اور ان باتوں سے فائدہ اٹھانا ہے یا پھر زندگی میں کہیں ٹھوکر کھا کر صرف افسوس ہی کرنا ہے، اُس وقت کا افسوس پھر کچھ فائدہ نہیں دیگی، اس لئے بہتر یہ ہے کہ آپ ابھی سے احتیاط کو اپنے زندگی کا لازمی حصہ بنائیں، یقیناً اس احتیاط میں بھی آپ کو صبر کے مراحل سے گزرنا ہوگا، انٹرنیٹ کی اسپیڈ سست ہوگی، اور ان کو اختیار کرنے میں بھی کافی وقت صَرف ہوگا مگر یہ کل کے افسوس سے بہتر ہے۔
لیکن یہ بات بھی ذہن میں رہے کہ حفاظت کرنے والا تو اللہ ہی ہے اور اس نے ہمیشہ اپنے بندوں کی حفاظت فرمائی ہے، جدید ترین ٹیکنالوجی بھی مجاہدین کا کچھ نہیں بگاڑ سکیں۔ مگر جو اسباب اللہ تعالیٰ نے ہمارے لئے مہیا کئے ہیں ہم ان اسباب کو اختیار کریں اور باقی اللہ پر توکل کریں۔ جب آسٹریلیا، امریکہ، فرانس میں مجاہدین کے کاروائیاں ہوتی ہیں اور اُدھر کی ایجنسی ان کا سراغ نہیں لگا سکتے تو ہماری ایجنسی جو کہ ان کا غلام ہے ہر لحاظ سے وہ کیا خاک معلوم کریگا۔ بس ہم غلطیاں نہ کریں، احتیاط کریں اور اصل کام اللہ پر توکل کریں تو یہ ہمارا کچھ نہیں بگاڑ سکتے۔

انٹرنیٹ کی دنیا پر مجاہدین اور اُن کے انصار کی بڑھتی ہوئی تعداد کو دیکھ کر خوشی ضرور ہوتی ہے لیکن یہ جان کر دکھ اور افسوس ہوتا ہے کہ اللہ اور اس کے رسول صلی اللہ علیہ وسلم کے واضح احکامات کے باوجود احتیاطی تدابیر اختیار کرنے میں اُن کی اکثریت خاصی سستی اختیار کرتی ہے۔ اور بارہا اس کے کافی سنگین نتائج سامنے آچکے ہیں۔

اسباب اختیار کرنے اور توکل سے متعلق بعض حضرات افراط و تفریط کا شکار ہیں، تو ضروری سمجھا یہاں مختصراً اس پہ بات کی جائے یعنی توکل ہے کیا اور اسباب اختیار کرنے کا حکم کیا ہے۔

التوکل: هو الإعتماد على الله و عدم الإلتفات الى ما عداه، قال السيد: هو الثقة بما عندالله و اليأس عما فى أيدى الناس۔ (قواعد الفقه ص: ۲۴۱ طبع صدف پبلشر)

یعنی توکل کے معنی اللہ تعالیٰ پر بھروسہ کرنے کے ہیں،اور بھروسہ کا مطلب یہ ہے کہ کام اسباب سے بنتا ہوا نہ دیکھے بلکہ یوں سمجھے کہ اسباب کے اندر مشیتِ الٰہی کی روح کارفرما ہے،اس کے بغیر تمام اسباب بیکار ہیں۔

توکل کے معنی ترکِ اسباب کے نہیں،بلکہ اسباب کو اختیار کرتے ہوئے اس کے نتائج کو اللہ کے حوالے کرنے کا نام توکل ہے لہذا اسباب کو اختیار کرو اور اس کے نتائج اور ثمرات کو اللہ تعالیٰ کے حوالے کرو،جیسا کہ حدیث شریف میں ہے کہ:

عن أَنَس بْن مَالِكٍ، يَقُولُ: جَاءَ رَجُلٌ إِلَى النَّبِيِّ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ، فَقَالَ: يَا رَسُولَ اللَّهِ، أَعْقِلُهَا وَأَتَوَكَّلُ، أَمْ أُطْلِقُهَا وَأَتَوَكَّلُ؟ قَالَ: «اِعْقِلْهَا وَتَوَكَّلْ» (ترمذى شريف : ۲۴۴۱)

ترجمہ:ایک صحابی نے نبی کریم صلی اللہ علیہ وسلم سے پوچھا کہ اے اللہ کے رسول! میں اپنے اونٹ کو باندھ کر اللہ پر توکل کروں یا اس کو چھوڑ دوں پھر اللہ تعالیٰ پر توکل کروں،تو نبی کریم صلی اللہ علیہ وسلم نے ارشاد فرمایا کہ:اونٹ کو باندھو،پھر اللہ پر توکل کرو۔

یہ واقعہ جامع ترمذی وغیرہ کتب حدیث میں موجود ہے۔

اس طرح آنحضرت صلی اللہ علیہ وسلم اور صحابہ کرام رضی اللہ عنہم نے اسباب اختیار فرمائے ہیں،بیماری میں علاج اختیار فرمایا ہے جیسا کہ ایک روایت میں آتا ہے کہ:

عن اسامة بن شريک قال: قالو يا رسول‌الله افنتداوى؟ قال: نعم يا عبادالله! تداووْ ، فان الله لم يضع داءاً إلا وضع له شفاء غير داء واحد الهرم۔ (مشكوة ۳۷۷/۲ ،ط: رواه احمد والترمذى و ابو داود)

ترجمہ:حضرت اسامہ بن شریک سے روایت ہے کہ صحابہ کرام رضوان اللہ علیہم اجمعین نے نبی کریم صلی اللہ علیہ وسلم سے دریافت کیا کہ اے اللہ کے رسول! (جب ہم بیمار ہوں تو) کیا ہم علاج کروائیں؟ تو جنابِ رسول اللہ صلی اللہ علیہ وسلم نے ارشاد فرمایا:اے اللہ کے بندو! ہاں علاج کرواو،کیونکہ اللہ تعالیٰ نے بڑھاپے کے علاوہ تمام بیماریوں کا علاج پیدا فرمایا ہے۔

سہل بن عبداللہ رحمہ اللہ علیہ نے فرمایا کہ جس شخص نے اسباب اخذ کرنے پر طعن کیا ہے تو گویا کہ اس نے سنت پر طعن کیا ہے اور جس نے توکل پر طعن کیا ہے تو گویا کہ اس نے ایمان پر طعن کیا ہے۔

آپ صلی اللہ علیہ وسلم کی بہت احادیث ہیں جس میں کام اور کمائی کرنے کا دعوت دیتے ہیں۔اسی طرح حضور صلی اللہ علیہ وسلم کی زمانہ مطہرہ میں اسکا عام طور پر مشاہدہ کیا گیا ہے کہ ہر غزوہ سے قبل جنگی سامان اور جنگی تیاری کا اہتمام فرماتے اور تمام اسباب کو مدنظر رکھتے تھے۔

اور لشکر کی سلامتی کیلئے ضروری احتیاطی تدابیر اختیار کرتے تھے۔اور اپنے فوج کی حفاظت فرماتے تھے۔

اور دشمن کے بارے میں معلومات حاصل کرنے کیلئے خفیہ طریقے سے لوگ بھیجواتے تھے۔اور اسکی کمزوری معلوم کرنے کا کوشش کرتے تھے۔اور جس نے آپ صلی اللہ علیہ وسلم کا سیرت اور غزوات مبارکہ پڑھ لیا ہے تو اسکی کیلئے یہ بات واضح ہو جاتا ہے کہ اسباب اختیار کرنا اللہ تعالیٰ پر توکل کرنے کا منافی ہونا لازمی نہیں۔بلکہ اسباب کا اختیار نہ کرنا نبی کریم صلی اللہ علیہ وسلم اور پہلے انبیاء علیہم السلام کے سنت کی خلاف ورزی ہے۔جیسا کہ نوح علیہ السلام نے اللہ تعالیٰ کے حکم کے مطابق کشتی بنایا تاکہ وہ خود کو اور اپنے ساتھ مؤمن

لوگ طوفان سے بچائے۔اسی طرح یعقوب علیہ السلام نے جب اپنے بیٹوں کو کہا کہ بد نظری سے بچنے کیلئے ایک دروازے سے مت داخل ہوں بلکہ مختلف دروازوں سے داخل ہونا،اس طرح کے اور کئی واقعات ہیں۔

اب آتے ہیں اسباب کی اقسام اور اُن کے احکام کی طرف۔۔

جو اسباب ناجائز اور غیر شرعی ہوں اُن کو توکلاً علی اللہ بالکل ترک کردے،اور جو اسباب جائز اور مشروع ہوں،ان کی تین قسمیں ہیں اور ہر ایک کا حکم الگ ہے:

ا۔مقطوع بہ۔۔یعنی وہ اسباب جن پر مسبّب کا مرتب ہونا قطعی ویقینی ہے یعنی وہ اسباب یقینی طور پر ضرر کو زائل کرتے ہوں اور ضرر بھی یقینی ہو، جیسے کھانا کھانا بھوک کیلئے، بھوک ضرر ہے جس سے موت بھی واقع ہونا قطعی ہے اور پانی پینا پیاس کیلئے،ان اسباب کا اختیار کرنا فرض ہے اور ان کا ترک کرنا حرام ہے۔(احتیاطی تدابیر اختیار کرنا اسی قسم سے ہے)

۲۔مظنون۔۔یعنی ظنی اسباب،یعنی وہ اسباب جو کبھی تو ضرر کو زائل کرتی ہوں اور کبھی نہ کرتے ہوں اور یہ ہوتے بھی انسان کے تجربات کے لحاظ سے یا سائنسی ایجادات کے لحاظ سے جیسے بیماریوں کے علاج کیلئے دوا وغیرہ،اس کا حکم یہ ہے کہ ہم ایسے کمزوروں کو ان اسباب کا ترک کرنا بھی جائز نہیں،البتہ جو حضرات قوتِ ایمانی اور قوتِ توکل میں مضبوط ہوں،ان کیلئے اسبابِ ظنیہ کا ترک جائز ہے۔

۳۔موہوم۔۔یعنی وہمی اور مشکوک اسباب یعنی جن کے اختیار کرنے میں شک ہو کہ مفید ہوں گے یا نہیں،ان کا اختیار کرنا سب کے لئے خلافِ توکل ہے، گو بعض صورتوں میں جائز ہے جیسے جھاڑ پھونک وغیرہ۔

(تفصیل کیلئے ملاحظہ ہو فتاوی ہندیہ جلد ۵،ص ۳۵۵،ناشر:دار الفکر)

جہاں تک اس حدیث کا تعلق جس کو لوگ دلیل پکڑ کر تمام اسباب کو ہی چھوڑ دیتے ہیں:

«يَدْخُلُ الْجَنَّةَ مِنْ أُمَّتِي سَبْعُونَ أَلْفًا بِغَيْرِ حِسَابٍ، لَا يَكْتَوُونَ، وَلَا يَسْتَرْقُونَ، وَلَا يَتَطَيَّرُونَ، وَعَلَى رَبِّهِمْ يَتَوَكَّلُونَ»

یعنی میری امت میں سے ۷۰ ہزار لوگ بغیر حساب کتاب کے جنت میں داخل ہونگے، یہ وہ لوگ ہیں جو نہ داغ دیتے ہیں،نہ جھاڑ پھونک کرتے ہیں،اور نہ فال نکالتے ہیں اور اپنے رب پر پورا بھروسہ رکھتے ہیں۔

تو اس حدیث میں استرقی اور اکتوی یہ موہوم اسباب میں شمار ہوتے ہیں اور الطیرۃ غیر شرعی وناجائز اسباب میں شمار ہوتا ہے

کیونکہ دوسرے حدیث میں آیا ہے

قَالَ رَسُولُ اللَّهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ: «الطِّيَرَةُ شِرْكٌ – ثَلَاثًا – وَمَا مِنَّا إِلَّا، وَلَكِنَّ اللَّهَ يُذْهِبُهُ بِالتَّوَكُّلِ»

اور استرقی اور اکتوی کے بارے میں صرف یہ فرمایا کہ

«مَنِ اسْتَرْقَى وَاكْتَوَى فَقَدْ بَرِئَ مِنَ التَّوَكُّلِ»

تو اس حدیث میں جن اسباب کو اختیار کرنے کا ذکر ہے وہ غیر شرعی یا وہمی اسباب ہیں جن کے متعلق ہم کہہ چکے ہیں کہ غیر شرعی کا تو اختیار کرنا جائز نہیں اور وہمی جیسے استرقی یعنی جھاڑ پھونک،تو اس کا اختیار کرنا جائز تو ہے مگر توکل کے خلاف ہے۔

اوراس حدیث میں بھی اُن کا ذکر ہے جو قوتِ ایمانی اور قوتِ توکل میں مضبوط ہوں،اسی لئے توفرمایا کہ میری امت میں سے صرف ۷۰ہزار بغیر حساب کتاب کے جنت میں داخل ہونگے،جو اللہ تعالی پر پورا بھروسہ رکھتے ہوں۔تو پورے امت میں سے یعنی صحابہ سے لیکر آخر زمانہ تک جتنے بھی لوگ ہونگے ان سب میں سے صرف ۷۰ہزار تو بہت کم ہیں،یہ ایک اعزازی انعام ہے اُن لوگوں کیلئے جو قوتِ ایمانی میں بہت آگے جاچکے ہوں۔

اور جہاں تک احتیاطی تدابیر کے اختیار کرنے کا مسئلہ ہے وہ یا تو مقطوع بہ اسباب میں شمار ہوتے ہیں یا زیادہ سے زیادہ مظنون میں،جن کے اختیار کرنے میں ثواب ہے ان شاءاللہ اور یہ توکل کے خلاف ہر گز نہیں ہے،بس نظریں ان اسباب پہ نہ ہوں کہ ان کو اختیار کر کہ کچھ نہ ہو گا بلکہ نظریں اللہ پر ہوں کہ وہی بچانے والی ذات ہے اور اسی نے ہی یہ اسباب پیدا کئے ہیں اور وہی بچائیگا،ان شاءاللہ۔

سیکشن اول۔۔۔۔۔۔۔۔۔۔۔۔۔

موبائل سیکیورٹی

نوٹ: جتنے بھی سافٹوئیر کے ٹوریئل بتائینگے آگے ان سافٹوئیر کے نئے ورشن میں ممکن ہے ڈیزائن مختلف ہو،اور جیسا تصویروں میں دکھایا ہے ویسا نہ ہو، مگر آپ اِس کو دیکھ کر اور سمجھ کر کریں تو دوسرے ورشن میں مشکل نہیں ہوگی۔

اینڈرائیڈ (Android) موبائل میں سیکیورٹی کے حوالے سے چند احتیاطی تدابیر

موبائل میں انٹرنیٹ کا استعمال خطرے سے خالی نہیں،اور وہ بھی جب کہ مجاہدین کے حوالے سے خبریں دیکھتے یا دیتے ہوں۔ تو اس سلسلے میں آپ کو بتاتا چلوں کہ کیا کیا بنیادی احتیاط کریں

سب سے پہلی بات کہ آپ کی لوکیشن اور آپ جو انٹرنیٹ پہ دیکھ رہے ہیں وہ دوسروں کی معلومات میں نہ آئے،یعنی آئی پی ایڈریس تبدیل کرنا اور انٹرنیٹ ٹریفک انکرپٹڈ کرنا۔۔۔

آئی پی ایڈریس چھپانے اور ڈیٹا انکرپٹ کرنے کیلئے ایف سیکیور فریڈوم کا استعمال۔۔۔

اس کیلئے سب سے بہترین سافٹوئیر تو "اُربوٹ" ہے مگر چونکہ اس کے تمام فنکشن روٹ والے موبائل میں ہی چلتے ہیں اس لئے ہم اس کا استعمال نہیں کرینگے۔اس کے بعد جو سب سے بہتر ہے وہ 'ایف سیکیور فریڈوم' ہے۔اس کے بہت زیادہ فائدے ہیں،لوکیشن ٹریس ہونے سے بھی بچاتا ہے۔

F Secure Freedome کو ڈاونلوڈ اور استعمال کرنے کا طریقہ:-

http://www.1mobile.com/f-secure-freedome-vpn-1550562.html

یا

https://play.google.com/store/apps/details?id=com.fsecure.freedome.vpn.security.privacy.android

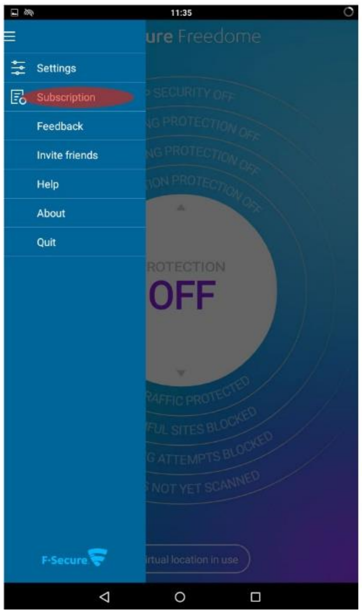
اس کو ان لنک کے ذریعے ڈاونلوڈ کر کہ انسٹال کریں۔شروع میں اس کا ٹوریئل آئیگا اس سے آپ کو اس کا استعمال آجائیگا۔

ویسے یہ سافٹوئر ۱۵ دن کے لئے فری ہے مگر اس کو دو کوڈ ڈالنے کے ذریعے اس کی مدت بڑھا سکتے ہیں،۱۲۰ دن تک چلے گا،کوڈ ڈالنے کا طریقہ

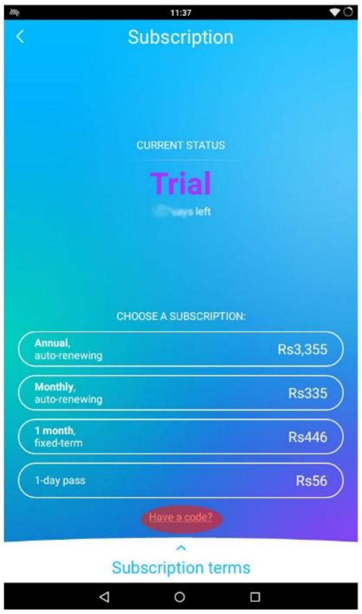
پہلا کوڈ یہ ڈالیں k4kc4m

1

2



3



جیسا تصویر میں دکھایا ہے ویسا کریں، یعنی پہلے ڈراپ مینیو یعنی تین لکیروں پہ کلک کریں پھر سبسکرپشن پہ اور پھر 'ہیوا ے کوڈ' پہ اور پھر وہ کوڈ لکھیں جو اوپر بتا چکا ہوں، ویسے جب شروع میں کھولتے ہو تو اس وقت بھی یہ آپشن آتا ہے، مگر اگر اس وقت نہیں کیا تو اس کا طریقہ یہی ہے۔

پھر دوبارہ یہی عمل کریں اور پھر یہ کوڈ ڈالیں w9f4ct اس سے آپ کو کل 120 دن استعمال کرنے کی اجازت مل جا ئیگی۔

چونکہ اس کا Pro ورژن کریک نہیں ہوا ہے اس لئے ہم یہ طریقہ کرتے ہیں۔

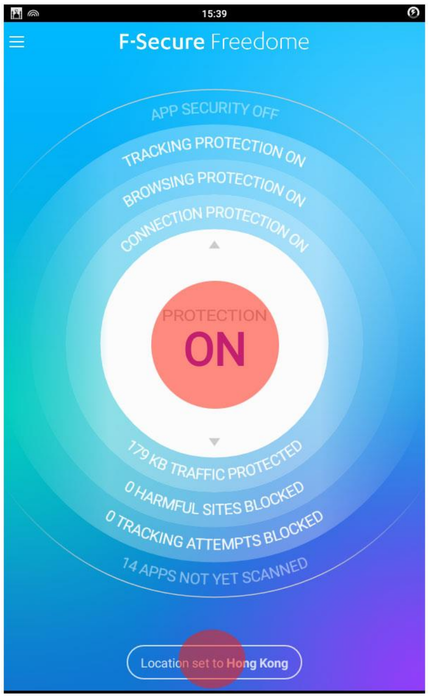
نوٹ:اس کوڈ کو ڈالنے کیلئے 'گوگل پلے اسٹور' پہ اکاونٹ کا ہونا ضروری ہے

اس کو سیٹ اور چلانے کا طریقہ:-اس کو پہلے ON کریں، اس کیلئے OFF پہ کلک کریں پھر ON لکھا آ ئیگا، پھر Location Set To پہ کلک کریں، پھر Other پہ کلک کریں اور پھر کوئی سا بھی ملک کا آئی پی ایڈریس استعمال کریں۔ امریکہ کا استعمال نہ کریں تو بہتر ہے

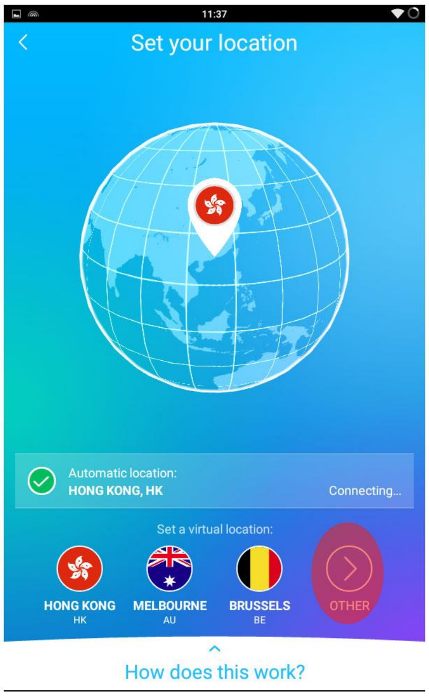
فیس بُک کیلئے ایک ہی ملک کا استعمال ہو تو بہتر ہے، اس لئے کہ بار بار ملک تبدیل کرنے سے فیس بُک سیکیورٹی سوال کریگا وہ اگر نہ آئے تو اکاونٹ بند ہو جایئگا۔

باقی طریقہ تصویر میں دیا ہے۔

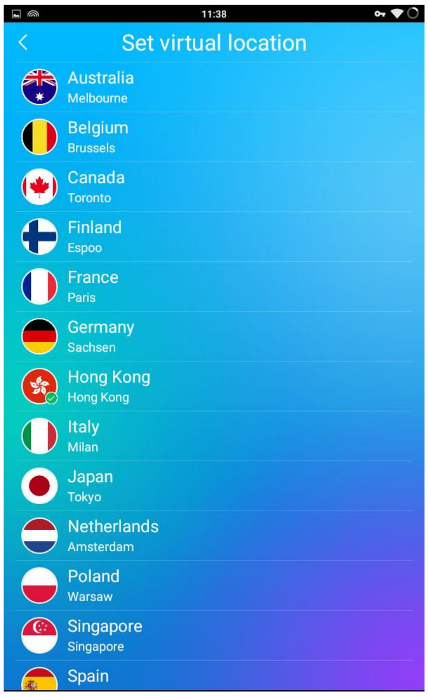
1



2



3



اب آپ کا آئی پی ایڈریس تبدیل ہو گیا اور ڈیٹا بھی انکرپٹڈ ہو گا، اور بمطابق اس کے آپ کا لوکیشن بھی ٹریس نہیں ہو گا اور یہ سافٹوئر تمام Apps کو خود ہی سرچ کریگا، یعنی جاسوسی سافٹوئیر اگر انسٹال ہوا اس کا سراغ لگائیگا۔ اب تمام موبائل کی نیٹ ٹریفک کسی حد تک محفوظ ہو گی۔

نوٹ: اس سے آپ کا فیسبوک والا پیکیج کا ڈیٹا استعمال نہیں ہو گا بلکہ عام نیٹ کا ڈیٹا استعمال ہو گا، اس لئے اس کے لئے نیٹ پیکیج ضروری ہے۔

اس کے 120 دن پورا ہو جانے کے بعد آپ دو طریقے کر سکتے ہیں ایک یہ کہ پچھلے تصویر میں دیکھیں جہاں سبسکرپشن سلکٹ کیا تھا وہاں Invite Friends پہ کلک کریں، ایک کوڈ نظر آئیگا وہ کوڈ آپ فیسبوک پہ شئیر کریں، جو بھی وہ کوڈ اپنے فریڈوم میں ڈالے گا اس کے 30 دن اور آپ کے 90 دن بڑھ جائینگے

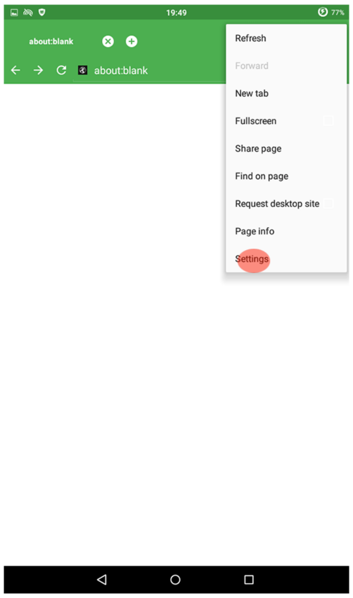
دوسرا طریقہ یہ ہے کہ اپنا موبائل فارمیٹ / فیکٹری ریسیٹ کریں۔ اس سے آپ کے موبائل کی تمام چیزیں ڈیلیٹ ہو جائینگی۔ اس کا طریقہ ہر موبائل میں مختلف ہے، یہاں صرف سیمسنگ کے اینڈرائڈ 5.1 کی مثال دیتا ہوں، سب سے پہلے settings میں جائیں پھر Backup & Reset میں جائیں، پھر Factory data Reset میں جائیں پھر Reset Mobile پہ کلک کریں۔ موبائل ریسیٹ ہو جائیگا۔ اور پھر دوبارہ یہ سافٹوئر انسٹال کریں اور دوبارہ وہی عمل کریں تو پھر سے آپ کو 120 دن ملیں گے۔

براوزر میں لوکیشن ٹریس والے آپشن کو ختم کرنا

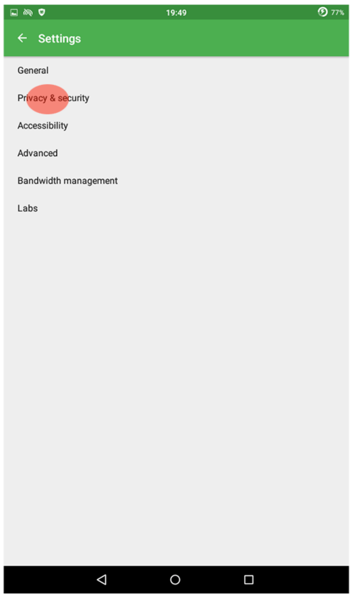
الف: اینڈرائیڈ براوزر میں اس کا طریقہ:

1

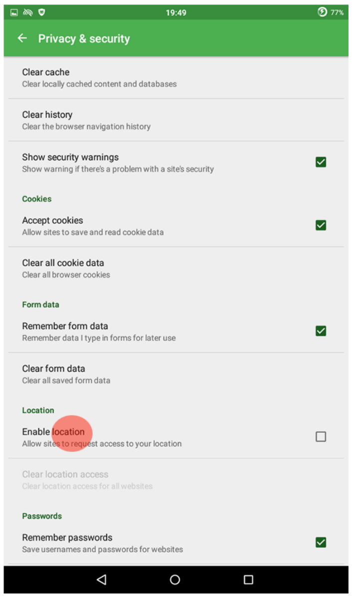
2



3



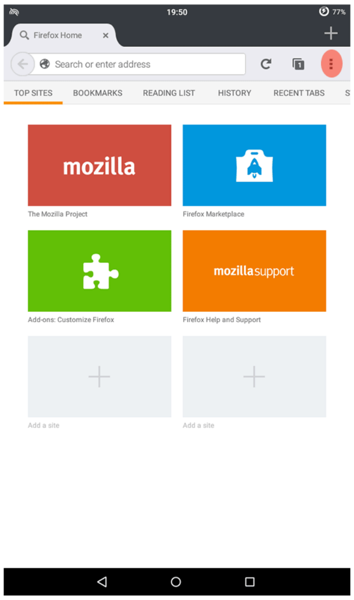
4



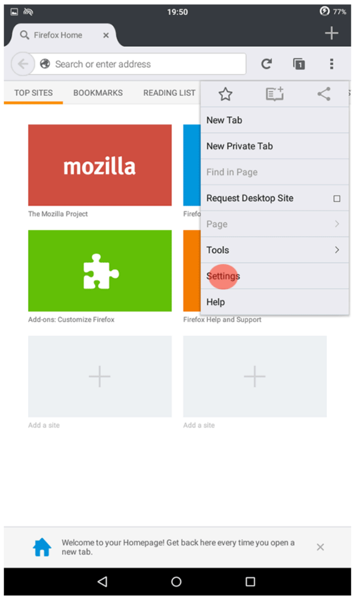
تصویر دیکھیں اور ویسا کریں اور Enable Location کے صحیح کے نشان کو ختم کریں

ب: فائر فوکس میں اس کا طریقہ:

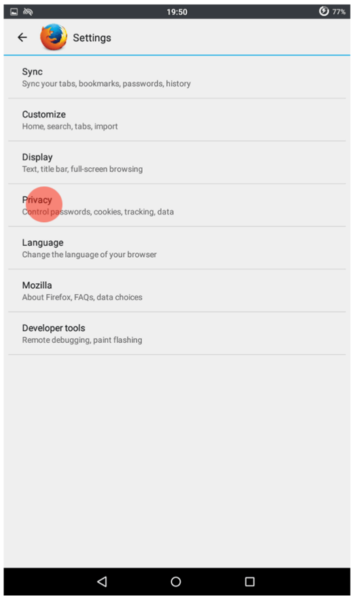
1



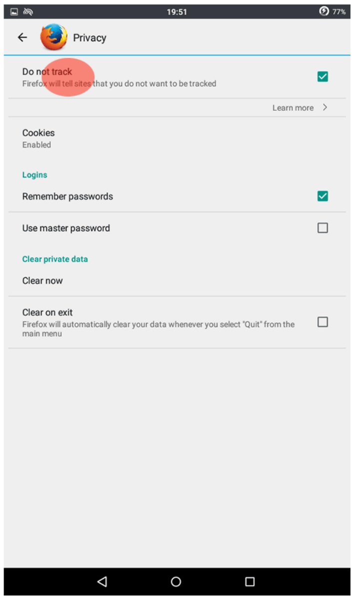
2



3

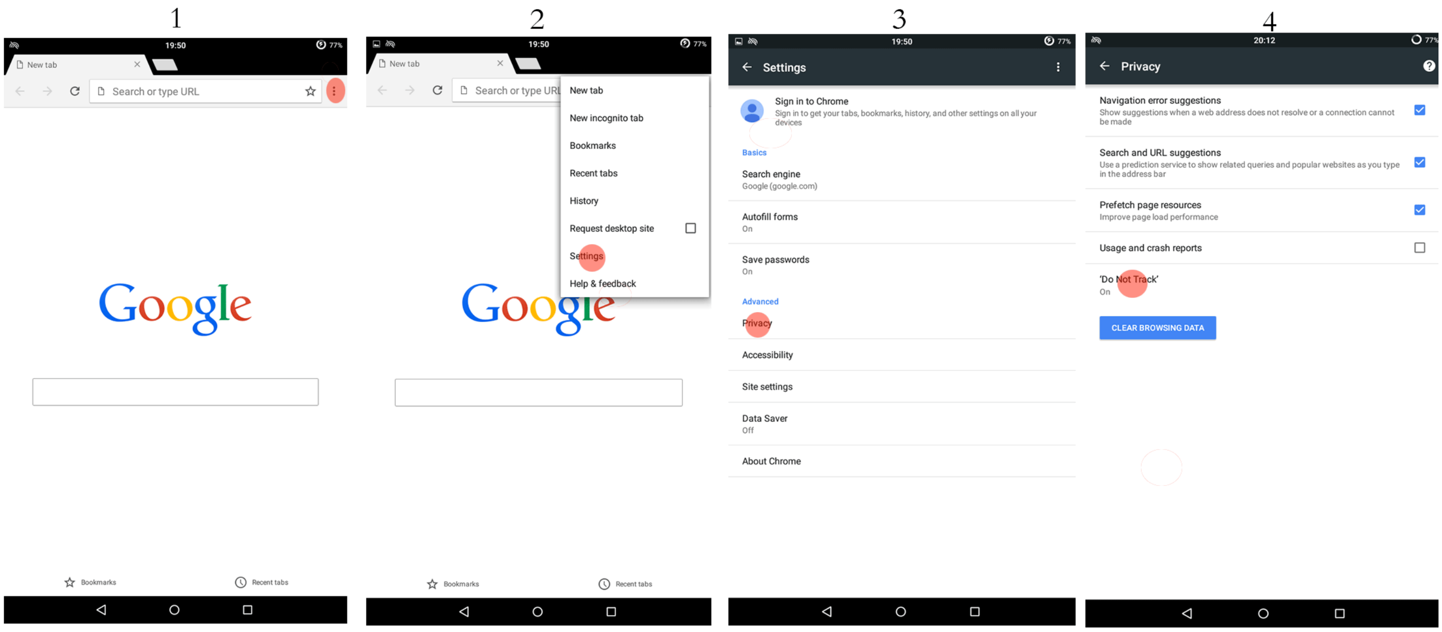


4



اس میں تصویر پہ عمل کریں اور آخر میں Do not track پہ صحیح کا نشان لگائیں

ج: گوگل کروم میں اس کا طریقہ:



جیسا تصویر میں دکھایا ہے ویسا کریں اور آخر میں Do not Track کو کلک کریں اور اسے ON کریں۔

براوزر کے دیگر احتیاط

فائرفوکس میں Privacy والے سیٹنگز کے خانے میں Cookies کو کلک کریں اور اسے Disable کریں، اور Clear on exit کو صحیح کا نشان لگائیں۔

اینڈرائیڈ براوزر میں Privacy & Security والے سیٹنگز کے خانے میں Accept cookies, Remember form data, Remember password والے آپشن کے صحیح کے نشان کو ختم کریں، یعنی ان کو بند کرنا ہے۔

کروم میں سیٹنگز میں جائیں، پھر Content settings میں جائیں اور وہاں Accept cookies, Enable location والے آپشن کے صحیح کے نشان کو ختم کریں

گوگل سے متعلق کچھ باتیں: گوگل اپنے صارفین کی مکمل معلومات حاصل کرنے کی کوشش کرتا ہے، بندے کو کیا پسند ہے کیا ناپسند، کس چیز میں دلچسپی ہے کس میں نہیں، کیا سرچ کر رہا ہے، کہاں ہے، کس شعبے میں ہے، اس طرح کے ذاتی معلومات وہ اپنے ایپس کے ذریعے اور سرچ انجن کے ذریعے سے معلوم کرتا ہے اور ان کا حکومتوں سے معاہدہ بھی ہے کہ دہشت گردی کی خلاف وہ حکومتوں کا ساتھ دینگے، تو کوشش کریں کہ گوگل کے ایپ اور اس کا سرچ انجن کو استعمال نہ کریں جب تک کہ ضرورت نہ ہو۔

براوزر کا سرچ انجن گوگل کے علاوہ دوسرا رکھیں

اینڈرائیڈ براوزر میں سیٹنگز میں جائیں پھر Advanced میں جائیں، پھر Set search engine پہ کلک کریں اور اس میں DuckDuckGo کو سیلکٹ کریں۔

فائرفوکس میں سیٹنگز میں جائیں، پھر customize میں جائیں اور وہاں سرچ انجن کو DuckDuckGo کو سیلکٹ کریں

گوگل کُروم میں سیٹنگز میں جائیں ،پھر سرچ انجن پہ کلک کریں، پھر اس میں yahoo یا Bing سیلکٹ کریں۔

Web RTC کا مسئلہ

آج کل یہ web RTC کا مسئلہ تمام براوزر میں ہے، کہ اس سے آپ کی اصل آئی پی ایڈریس ظاہر ہوتی ہے آپ چاہے جونسا بھی پراکسی سافٹوئیر استعمال کررہے ہوں چاہے وہ F Secure Freedome ہو یا Hotspot shield مگر آپ کی اصل آئی پی تب بھی ظاہر ہوسکتی ہے۔اس کو کمپیوٹر کے براوزر میں تو ختم کرنا آسان ہے مگر موبائل میں Firefox کے علاوہ دوسروں میں اس کو ختم نہیں کرسکتے۔اینڈرائڈ براوزر، UC Browser، گوگل کُروم، Opera Browser، وغیرہ تمام میں یہ چیز موجود ہے، البتہ Opera Mini میں یہ چیز موجود نہیں ہے۔

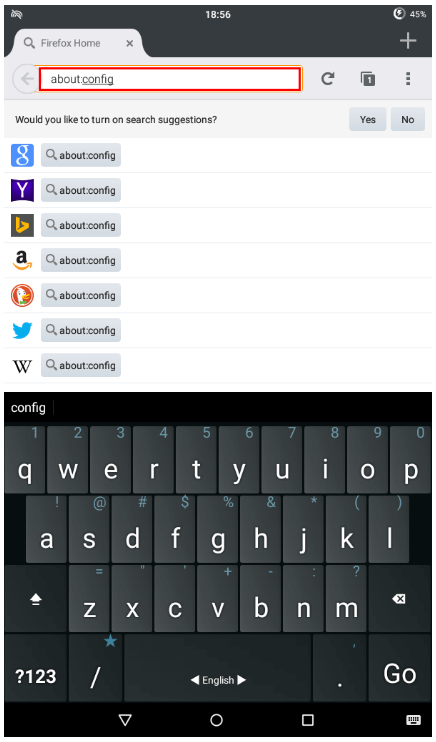
توآپ یا Opera Mini استعمال کریں یا Firefox ان کے علاوہ کوئی بھی براوزر جہادی ویب سائٹ کیلئے استعمال نہ کریں۔

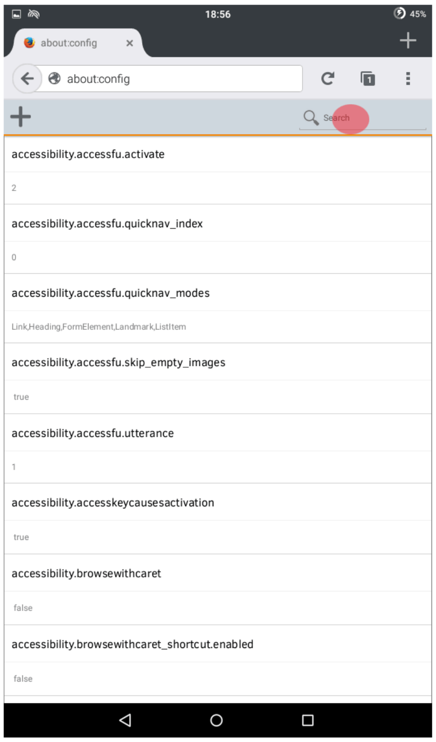
الف۔ Firefox میں web RTC کو ختم کرنے کا طریقہ:

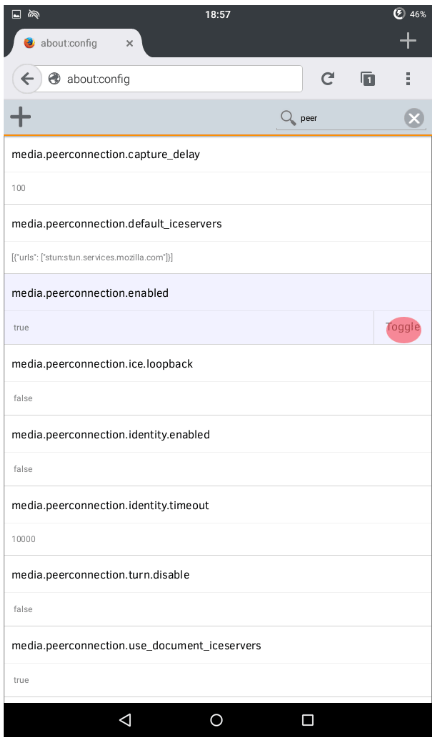
Firefox کھولیں اور ویب سائٹ لکھنے کی جگہ پر لکھیں:

about:config

جیسے نیچے تصویر میں دکھایا ہے۔







پھر سرچ میں لکھیں

media.peerconnection.enabled

اس پہ True لکھا ہوگا، اس میں Toggle پہ کلک کریں اور اب False لکھا ہوا نظر آئیگا، یعنی اب یہ webRTC کو آپ نے بند کر دیا ہے۔

یہ چیک کرنے کیلئے کہ واقعی بند ہو گیا ہے آپ اس لنک سے دیکھ سکتے ہیں، اگر اس میں پبلک آئی پی ایڈریس ظاہر ہو تو سمجھیں کہ بند نہیں ہوا، اگر پبلک آئی پی ایڈریس میں کچھ لکھا ہوا نہ ہو تو بند ہو چکا ہے۔

چیک کرنے کا لنک: https://diafygi.github.io/webrtc-ips

ویسے گوگل کروم میں اس کو بند کرنے کا ایک طریقہ ہے مگر وہ کام نہیں کرتا، وہ بھی بتا دیتا ہوں شاید کہ کام کرے آپ کے موبائل میں

گوگل کروم میں اس کا طریقہ: ویب سائٹ لکھنے کی جگہ پر یہ لکھیں chrome://flags/#disable-webrtc

پھر اس میں Enable پہ کلک کریں اور اپنا براوزر بند کر کے دوبارہ کھولیں۔ اور چیک کرنے کیلئے اسی لنک پہ جائیں جو اوپر بتا چکا ہوں۔

لوکیشن یا دوسرے اہم معلومات کے Permissions کو ختم یا محدود کرنا

چونکہ اکثر Apps کی Permission میں لوکیشن، کیمرہ، آڈیو ریکارڈنگ وغیرہ کا ذکر ہوتا ہے اور ہم بغیر دیکھے انسٹال کر لیتے ہیں جس کا مطلب یہ ہوتا ہے کہ یہ سافٹویئر اب آپ کی مرضی کے بغیر بھی آپ کے موبائل کا لوکیشن، کیمرہ کا استعمال، اور آڈیو ریکارڈنگ، کنٹیکٹس کی لسٹ، وائی فائی کا نام وغیرہ اہم معلومات حاصل بھی کر سکتا ہے اور دوسروں کو دے بھی سکتا ہے۔ اور اب جب فیس بک اور گوگل والوں نے اعلان کیا ہے کہ وہ دہشت گردوں کے خلاف حکومت کا مکمل ساتھ دینگے تو اس کو زیادہ اہمیت حاصل ہے اور اس کو ضرور محدود کریں

الف:APK Permission Remover:

ایک سافٹویئر ڈاونلوڈ کرنا ہوگا جس کا نام APK Permission Remover ہے، اسکا Pro ورشن ڈاونلوڈ کریں تو زیادہ بہتر ہوگا،

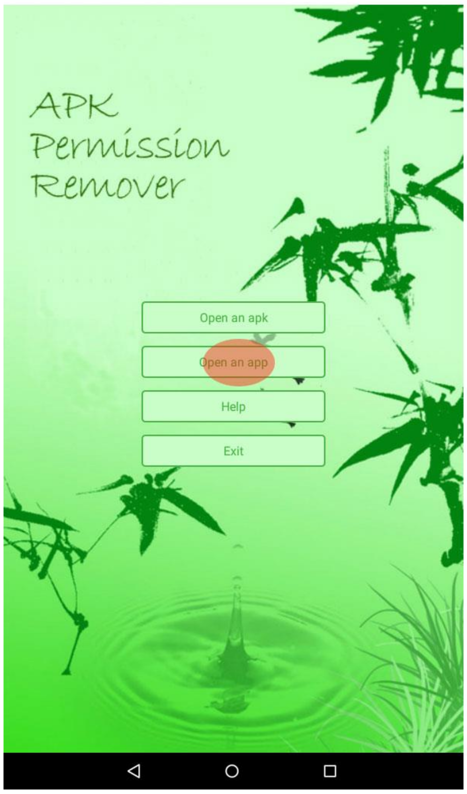
فری ورشن کا لنک: https://play.google.com/store/apps/details?id=com.gmail.heagoo.apkpermremover

یا

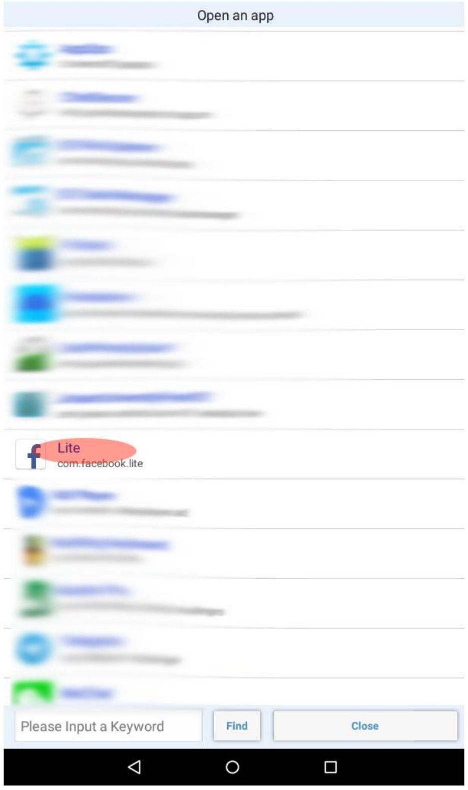
http://www.1mobile.com/apk-permission-remover-1314082.html

ڈاونلوڈ کرنے کے بعد اس کو کھولیں،

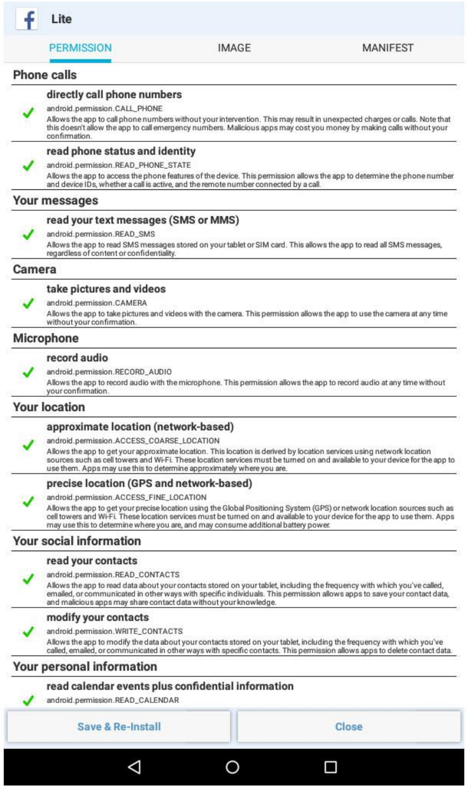
1



2



3



ہمارے سافٹویئر چونکہ پہلے سے انسٹال ہیں اس لئے ہم open an app پہ کلک کریں

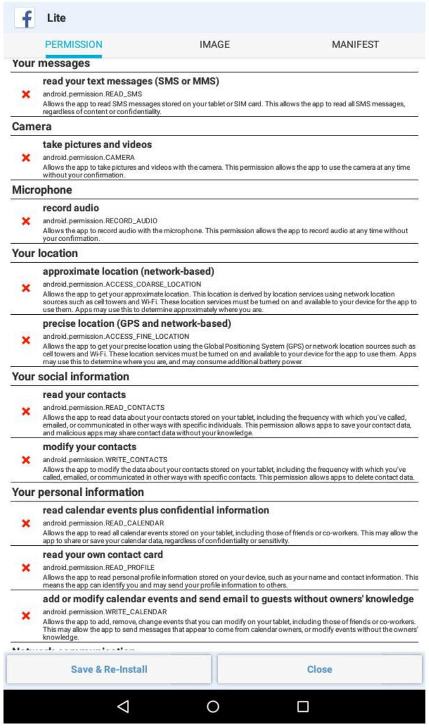
پھر جس سافٹویئز/ایپ کی پرمیشن محدود کرنی ہیں اس کو سلکٹ کریں

کرنا تو سب کو ہوگا جو بھی انسٹال ہوں تاکہ ان میں سے کوئی بھی آپ کی لوکیشن وغیرہ تک رسائی حاصل نہ کرسکے، اور چونکہ بعض ایپ دوسرے ایپ کے بارے میں اور اس کے اکاونٹ کے بارے میں پرمیشن لیتے ہیں اس لئے ان سب کو محدود کرنا ہوگا

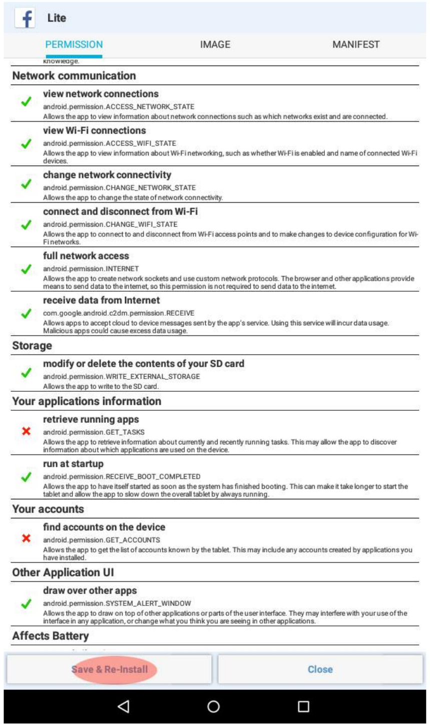
تصویر میں صرف فیسبوک لائٹ کا مثال دیا ہے، اس سے باقیوں کا بھی آپ اندازہ لگا سکتے ہیں۔

ایک ایپ سلکٹ کرلیں، پھر اس کے پرمیشن کا لسٹ کھلے گا، اس میں سے مندرجہ ذیل کو غلط کا نشان لگالیں، جیسا کے نیچے تصویر میں دکھایا ہے۔ صرف ان کو چھوڑلیں جو اس ایپ کی ضرورت ہوں باقی تمام کو ختم کردیں۔

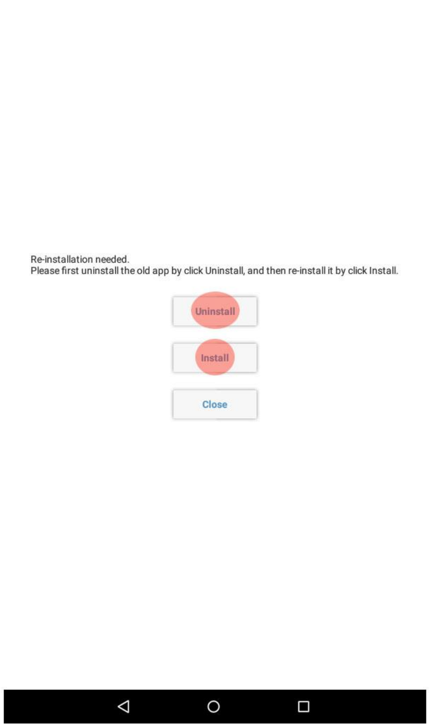
1



2



3



جب غیر ضروری چیزوں کو غلط کا نشان لگالیا ہو تو پھر Save & Re install پہ کلک کریں، اور پھر Uninstall کرکہ Install پہ کلک کریں

اس عمل سے اکثر کسی بھی ضروری چیز کو غلط کا نشان لگانے سے ایپ نہیں چلتا، اور اس کی بہت شکایات آئی ہیں تو بہتر یہی ہے کہ جو ایپ انسٹال نہ ہوں ان کے APK فائل کے ذریعے یہی عمل کریں یعنی شروع میں Open an App کی جگہ Open an APK پہ کلک کریں اور APK کو براوز کریں، باقی عمل یہی ہے۔

اگر APK موجود نہیں تو آپ Es File Explorer یا Zapya کے ذریعے اپنے انسٹال شدہ ایپ کو بیک اپ کرکہ ان کے APK بنا سکتے ہیں۔

APK فائل کو ویسے بھی کھولیں تو APK Permission Remover سے open ہونے کا آپشن آئیگا، اس سے بھی اوپن کرکہ پرمیشن ختم کرکہ انسٹال کرسکتے ہیں۔

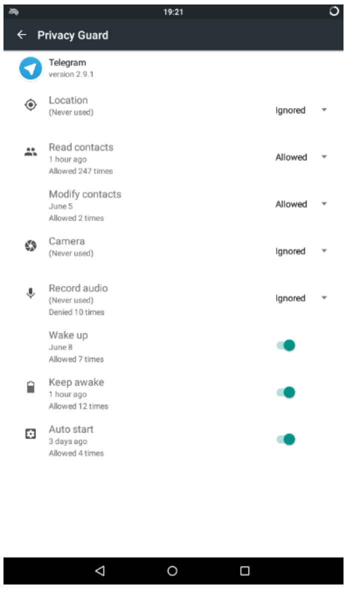
نوٹ:ایک اہم کمزوری اس ایپ کی یہ ہے کہ سیسٹم کے ایپ کے پرمیشن کو محدود نہیں کر سکتا، مثلاً گوگل پلے اسٹور، گوگل پلس وغیرہ۔

اوراس کے علاوہ whatsapp کا GPS location کو غلط کا نشان لگانے سے بھی میں مسئلہ آرہا بہت سے موبائل میں، کہ پھر وہ نہیں چلتا۔ **اس ایپ کا متبادل آگے بتائینگے۔**

جب آپ گوگل کے Apps استعمال کریں تو فوراً اکاونٹ لاگ آوٹ کرلیں وہ بھی موبائل کے settings میں جاکر جہاں اکاونٹ لکھے ہوتے ہیں وہاں سے ڈیلیٹ کرلیں اور بہتر تو یہی ہے کہ گوگل کا کوئی بھی اکاونٹ نہ بنائیں لیکن کچھ مجبوری ہوتی ہیں مثلاً اوپر F secure Freedome میں بتایا کہ وہ بھی بغیر گوگل کے اکاونٹ کے کوڈ نہیں ڈال سکتے، تو ایسے مجبوریوں میں یہی کریں کہ کام ہو جانے کے فوراً بعد اکاونٹ لاگ آوٹ کریں۔

ب: APK Permission Remover کا متبادل:

اس کیلئے موبائل کا روٹ ہونا ضروری ہے، ممکن ہے روٹ کے بغیر چل جائے مگر روٹ میں زیادہ کارگر ہے۔ روٹ کے بارے میں آگے بتائینگے۔ موبائل کو روٹ کرنے کے بعد Kit Kat یا lollipop ورشن میں آپ Appops نامی سافٹویئر ڈال لیں اس سے آپ تمام انسٹال شدہ Apps کی پرمیشن کو modify کر سکتے ہیں اور آرام سے تبدیل کر سکتے ہیں، اور سیسٹم کے ایپ کی پرمیشن بھی تبدیل کر سکتے ہیں۔



بس یہ انسٹال کرکہ کھولیں اور پھر اپنے موبائل کے Settings میں جائیں پھر Apps/Apps Manager پھر کوئی سا بھی ایپ سلکٹ کریں پھر اس کے Permissions کو Modify پہ کلک کریں، اور تمام غیر ضرور پیرمیشن کو Ignore پہ رکھیں۔ جیسے اس تصویر میں دکھایا گیا ہے۔

یہ صرف ایک کوڈنگ ہوتا ہے، اس لئے جب آپ اس ایپ کو کھولیں گے تو وہ اپنا کام کریگا بعد میں اس کو کھولنے کی ضرورت نہیں ہوگی۔

یہ اوپر والے ایپ کا متبادل اور اس سے بہتر کام کرتا ہے مگر چونکہ یہ اکثر بغیر روٹ والے اور 4.3 سے کم والے میں مسئلہ کرتا ہے، نہیں چلتا اس لئے اُس ایپ کو مقدم کیا کہ وہ غالباً سب میں چلتا ہے۔

لنک: https://play.google.com/store/apps/details?id=it.lorenzoff.appops

یا

http://www.1mobile.com/appops-2532553.html

اگر یہ نہ چلے آپ کے اینڈرااڈورشن میں تو آپApp opsنامی دوسرے سافٹویئر آزمالیں،کوئی نہ کوئی چلے گا،اور طریقہ کار سب کا یہی ہے۔
اور ممکن ہے کوئی ایسا بھی ہو جو اینڈرائڈ 4.3 سے کم پر بھی چلے بغیر روٹ کے۔
مقصد آپ کو پرمیشن ختم کرنے کا بتانا ہے چاہے جس بھی سافٹویئر سے کریں۔باقی کچھApp ops نامی سافٹویئر کے لنک یہ ہیں

https://play.google.com/store/apps/details?id=com.findsdk.apppermission

https://play.google.com/store/apps/details?id=fr.slvn.appops

https://play.google.com/store/apps/details?id=droidmate.appopsinstaller

نوٹ: آج کل کچھ نئے موبائل میں پرمیشن کو ختم کرنے کے لئے پہلے سے ہی سافٹویئر موجود ہیں۔اور اینڈائڈ کے نئے ورشن M arshmallow میں یہ سیٹنگز پہلے سے موجود ہیں۔

Root/روٹ

روٹ کو دوسرے الفاظ میں فلیش یا جیل بریک کہتے ہیں، یعنی یہ ایک ایسا طریقہ ہے جس سے کمپیوٹر سے موبائل کو فلیش کیا جاتا ہے جس کے بعد موبائل کے تمام پابندیوں کو آپ ہٹا کر موبائل کے آپریٹنگ سیسٹم کو اپنی مرضی کے مطابق کر سکتے ہیں، اس کے بہت سے فوائد و نقصانات ہیں، فائدے بعد میں ذکر کرینگے۔ نقصانات یہ ہیں کہ موبائل کا آپریٹنگ سیسٹم خراب ہونے کا خطرہ ہے مگر ۵ فی صد۔ مثلاً لائٹ ڈِم ہو جائے، یا تیز ہو جائے یا رنگ میں فرق آجائے وغیرہ۔ موبائل کی گارنٹی اور لائسنز بھی ختم ہو جاتی ہے۔

لیکن ہم آپ کو ایک محفوظ طریقے سے روٹ کرنے کا طریقہ بتائینگے، جس میں بغیر کمپیوٹر کے صرف موبائل سے ہی روٹ کرنا بتائینگے۔ مگر اس طریقے سے روٹ کرنے کے وقت انٹرنیٹ ضروری ہے۔

الف: موبائل سے روٹ کرنے کا طریقہ

اس کے لئے آپ ایک ایپ ڈاونلوڈ کرکہ انسٹال کرلیں جس کا نام Kingroot ہے، چونکہ یہ غیر قانونی ہیں اس لئے گوگل پلے اسٹور سے یہ آپ کو نہیں ملے گا۔

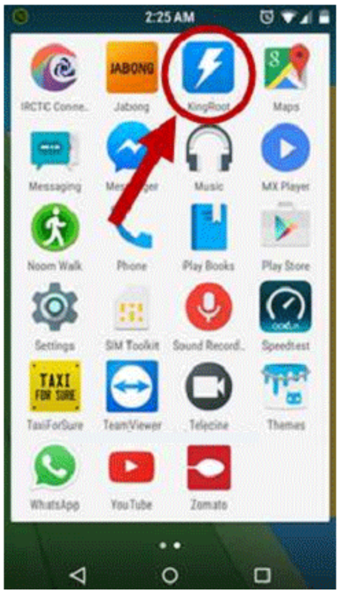
اس کا نیا ورشن 4.5 ہے اور اس کا لنک یہ ہے:

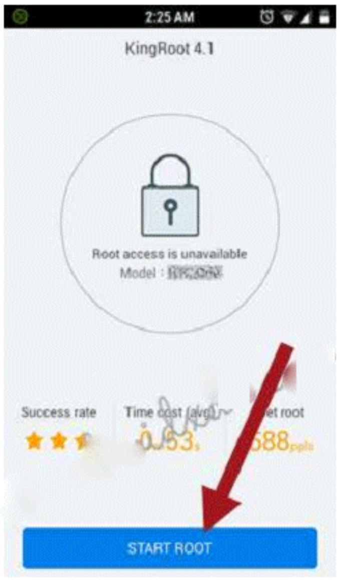
https://sites.google.com/site/androidxdacom/file/Kingroot_V4.5.0.722.apk?attredirects=0

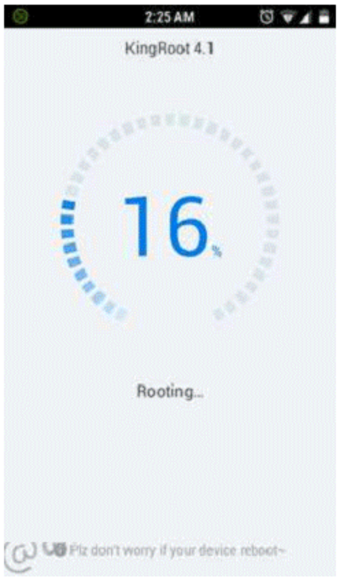
اور اس کے اگر اپڈیٹڈ ورشن دیکھنا ہو تو اس کے ویب سائٹ پر آپ دیکھ سکتے ہیں، مگر وہ چائینیز زبان میں ہے۔ ویب سائٹ کا لنک:

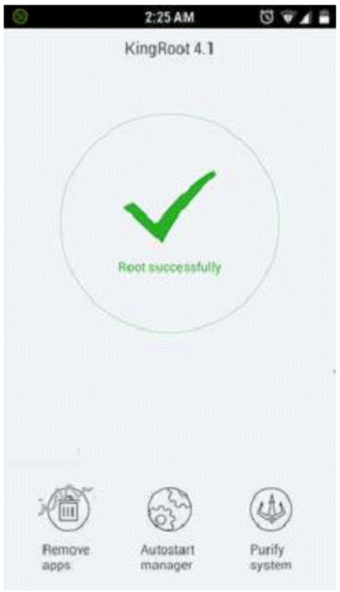
http://www.kingroot.net/release

پھر ڈاونلوڈ کرکہ انسٹال کریں، اور انسٹال کرنے کے بعد آپ اسے کھولیں تو یہ اسکرین آئیگا









تو آپ Start Root پہ کلک کریں، ۳ سے ۸ منٹ لگینگے انٹرنیٹ کے اسپیڈ کے مطابق ہوگا۔ اور اس درمیان میں ایک دو دفعہ فون بند ہو کہ دوبارہ اسٹارٹ ہوگا تو اس سے پریشان نہ ہوں۔

پھر جب ہو جائیگا تو Root Successfully لکھا آئیگا، اب آپ کا موبائل روٹ ہو چکا ہے۔

ممکن ہے انٹرنیٹ کے سستی کی وجہ سے ایک دفعہ میں نہ ہو تو آپ دو تین دفعہ کوشش کریں۔

اگر پھر بھی نہ ہو تو آپ کمپیوٹر سے کوشش کریں، کمپیوٹر سے روٹ کرنے کا طریقہ تھوڑا تفصیلی ہے۔

ب: کمپیوٹر سے روٹ کرنے کا سب سے آسان طریقہ:

ا۔ کمپیوٹر میں Root Genius نامی سافٹویر ڈاونلوڈ کریں۔ اس کے لیٹسٹ ورژن آپ یہاں سے ڈاونلوڈ کر سکتے ہیں:

http://androidxda.com/download-root-genius-application

ویسے اب تک جو سب سے نیا ورژن ہے وہ 2.3 ہے اور اس کا لنک یہ ہے:

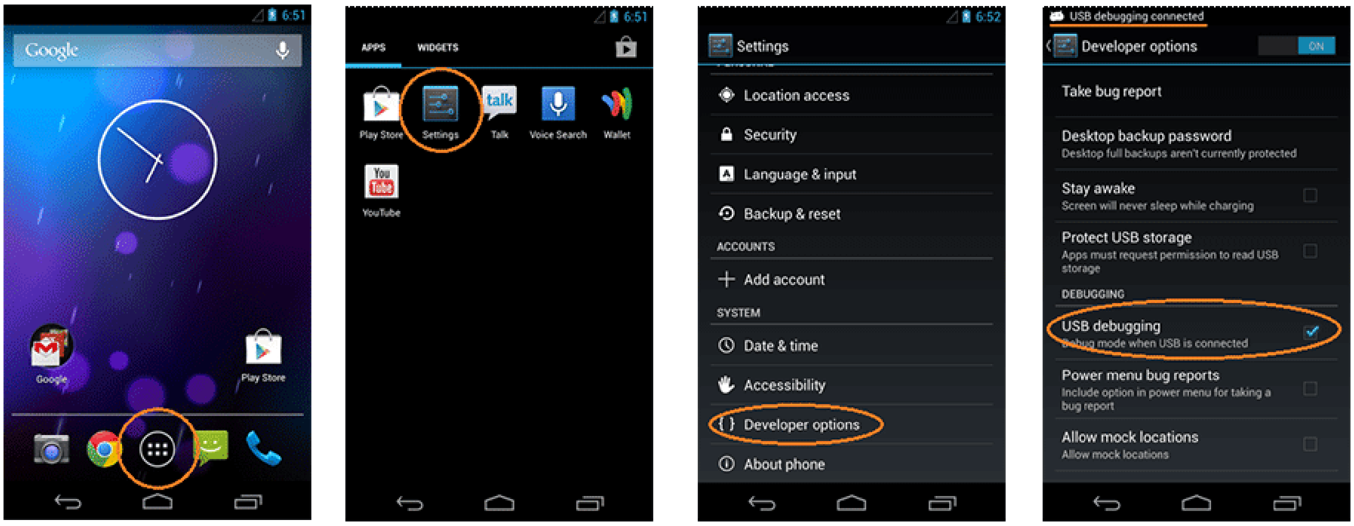
http://www.mediafire.com/download/j17ivciz1x808wo/RootGenius_v2.3.0.zip

یہ ڈاونلوڈ کریں اور اسے Unzip کریں۔

۲۔ موبائل کے ڈرائورز: پھر اپنے موبائل کے ڈرائورز / drivers اپنے کمپیوٹر میں ڈالیں تاکہ جب آپ اپنا موبائل کمپیوٹر پہ لگائینگے تو وہ اسے ڈیٹکٹ۔ اگر آپ کا موبائل سیمسنگ ہے تو آپ اپنے موبائل کا ماڈل یہاں تلاش کریں اور ڈاونلوڈ کر کہ انسٹال کریں: http://androidxda.com/download-samsung-usb-drivers

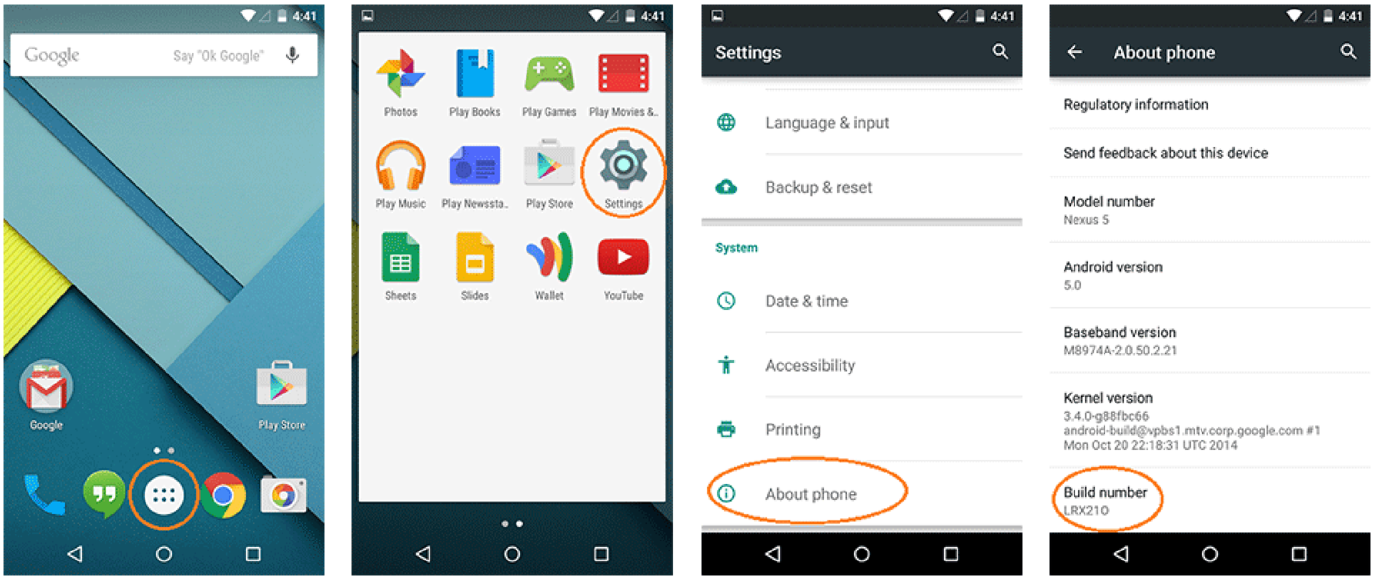
اور اگر Q Mobile ہے تو یہاں سے: http://androidxda.com/download-qmobile-usb-drivers

۳۔ موبائل میں USB Debugging کو Enable کرنا: اگر آپ اینڈرائڈ کا 4.2 سے کم والا ورژن استعمال کر رہے ہیں تو یہ تصویر ملاحظہ فرمائیں

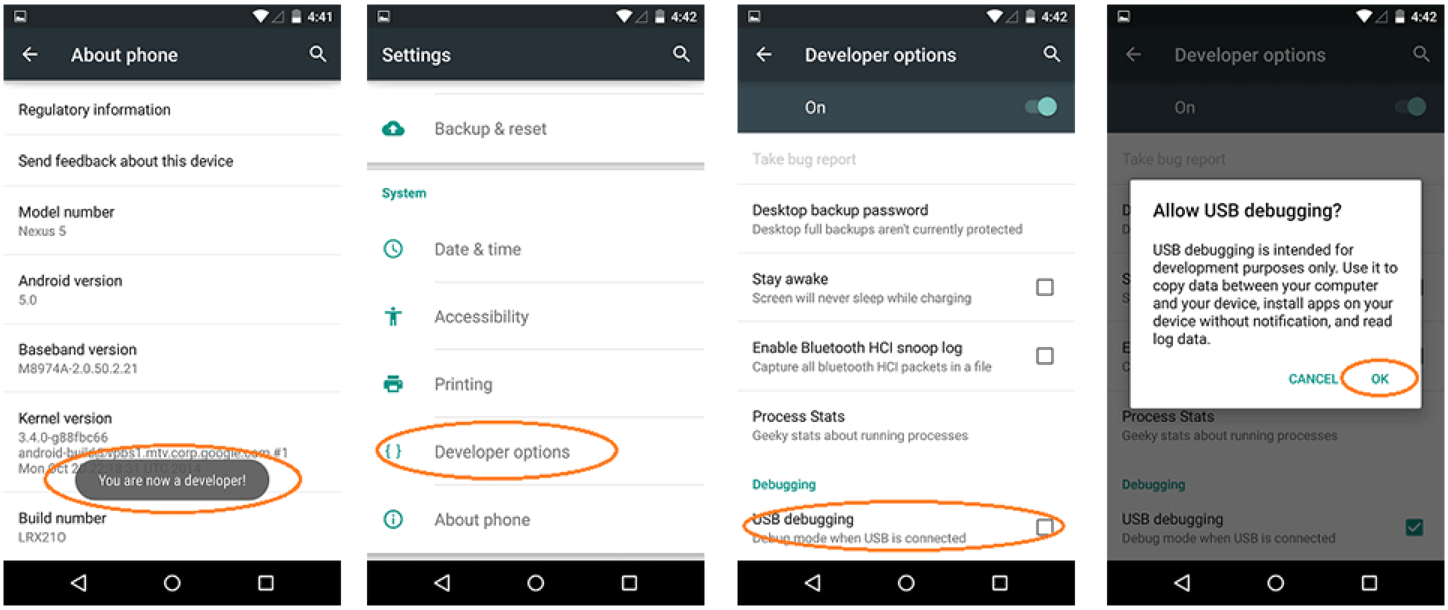


اگر Developer Options پہلے سے Off ہوتو اسے پہلے On کریں، پھر USB debugging کو صحیح کا نشان لگائیں۔

اینڈرائڈ 4.2 سے 5.1 والے، اگر آپ کے موبائل میں Developer options نہیں ہے تو نیچے تصویر پہ عمل کریں

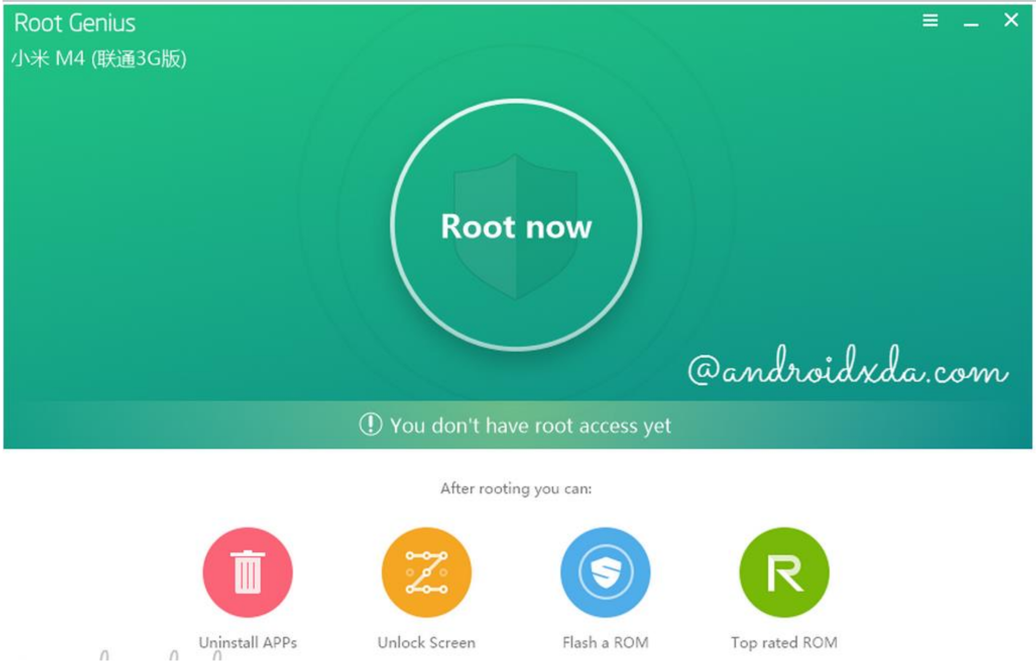


یعنی سیٹنگز میں جائیں پھر About phone میں جائیں پھر Build number کو 8 سے 10 مرتبہ دبائیں یہاں تک کہ You are now a developer لکھا آئے۔ جیسا نیچے تصویر میں دکھایا ہے۔



پھر Developer options پہ کلک کریں اور پھر USB debugging پہ کلک کریں اور پھر Allow USB Debugging کو Ok کریں۔

۴۔آخری مرحلہ:اب آپ Root Genius سافٹوئیر کھولیں اور اپنا موبائل کمپیوٹر پہ لگائیں،اگر آپ نے سارے کام صحیح طریقے سے کئے ہیں تو یہ اسکرین آئیگا

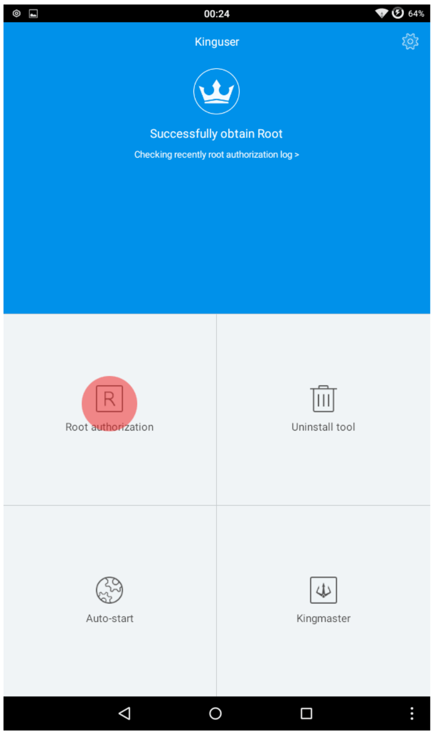


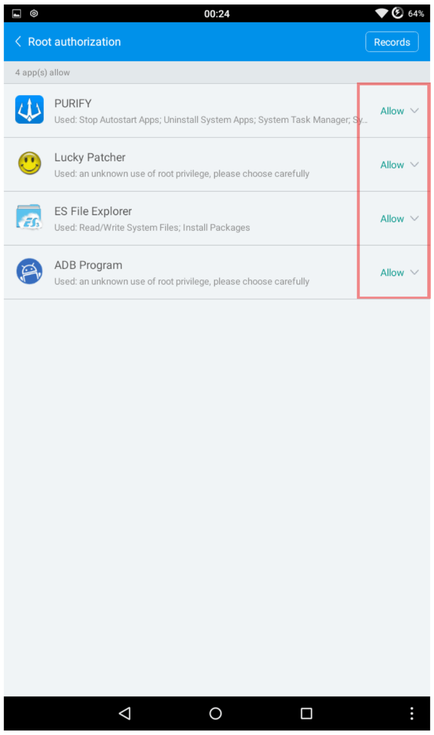
بس اب Root Now پہ کلک کریں،۵منٹ لگینگے اور آپ کا موبائل روٹ ہو جائیگا۔اگر اب بھی نہ ہو سکے تو دکاندار سے کرالیں۔

نوٹ: روٹ کرنے کے بعد آپ اپنے موبائل میں اینڈرائیڈ کا کوئی بھی ورشن ڈال سکتے ہیں،مگر یہ خود نہ کریں کسی دکاندار سے کروائیں،کیونکہ اس سے ممکن ہے آپ سے صحیح نہ ہو سکے اور آپریٹنگ سیسٹم خراب ہو جائے۔

روٹ کرنے کے بعد کی چیزیں

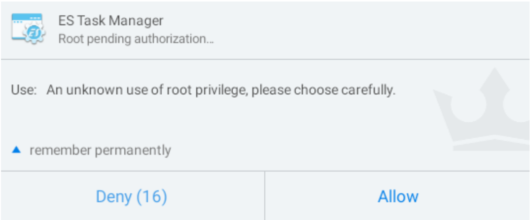
الف: روٹ کرنے کے بعد آپ کے موبائل میں ایک ایپ ہوگا Kinguser کے نام سے جو وہی Kingroot ہی ہے، آپ اسے کھولیں اور وہاں سے آپ دوسرے ایپ کو روٹ کی پرمیشن دے سکتے ہیں، اس تصویر کو دیکھ لیں





اس میں Root Authorization پہ کلک کریں اور پھر اُن ایپ کی لسٹ کھلے گی جو روٹ چاہتے ہیں آپ انہیں یہاں سے Allow کر دیں۔

یا اگر آپ انہیں یہاں سے Allow نہ بھی کریں تو آپ اُن ایپ کو کھول کر بھی Allow کر سکتے ہیں مثلاً اس تصویر کو دیکھ لیں۔



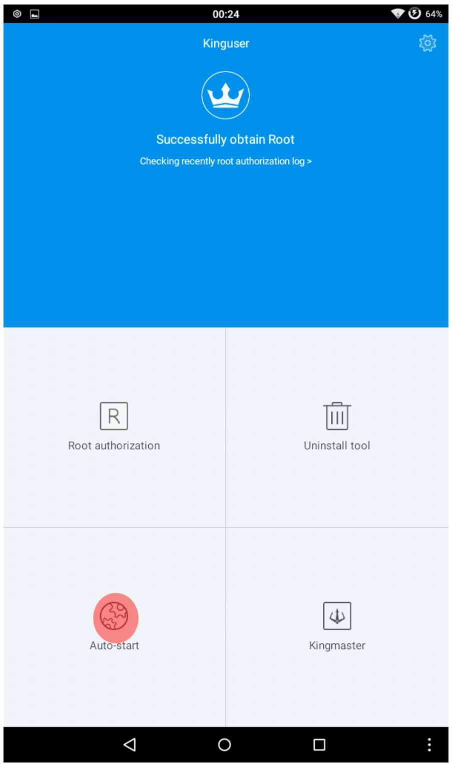
یعنی جب آپ اس ایپ کو کھولیں گے جو روٹ چاہتا ہے، کھولنے کے فوراً بعد یہ اسکرین آئیگا، اس میں اس کو Allow کر دیں.

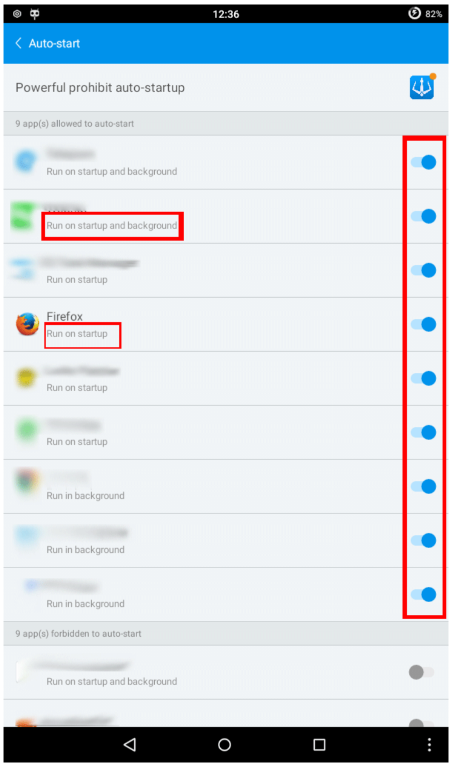
ب:بیک گراونڈ/ Background میں چلنے والے ایپ کو KingUser کے ذریعے بند کرنا: اینڈرائڈ میں جب آپ کسی ایپ کو بند کرتے ہیں تو وہ مکمل بند نہیں ہوتا، جیسے اس کی مثال یہ کہ آپ نے Whatsapp کھولا اور بند کیا مگر جب ایک میسج آتا ہے تو نوٹیفیکیشن میں آپ کو بتا دیتا ہے کہ whatsapp کا میسج آیا ہے حالانکہ آپ نے Whatsapp بند کیا ہوا تھا۔

تو ایپ بیک گراونڈ میں چل رہے ہوتے ہیں۔ان سے نقصان یہ ہے کہ جب آپ فیسبوک پہ فیک آئی ڈی بناتے ہیں اور whatsapp آپ کا اپنے نمبر پہ ہے، تو آئی پی ایڈریس چینج کر کہ آپ فیسبوک کی آئی ڈی استعمال کر رہے ہوں تو ساتھ Whatsapp بھی چل رہا ہوتا ہے، جو کہ آپ اپنی اصل آئی پی ایڈریس سے استعمال کر چکے ہیں ۔اس سے اگر کوئی آپ کو ٹریس کرنا چاہ رہا ہے تو آسانی سے ٹریس کر سکے گا کہ یہ آپ ہی ہیں۔

تو جب آپ فیک آئی ڈی استعمال کر رہے ہوں تو بیک گراونڈ میں وہ تمام ایپ کو بند کر دیں جس میں آپ کی اصل شناخت کی معلومات ہیں۔اس کے لئے اگر آپ کے موبائل میں AppOps صحیح انسٹال ہوا تھا تو آپ اس کے ذریعے بھی کر سکتے ہیں اس میں Modify میں wake up, keep awake, autostart کے پرمیشن کو ختم کر دیں۔

اس سے بہتر اور زیادہ موئثر طریقہ Kinguser سے ختم کرنا ہے اس کا طریقہ یہ ہے، جیسے تصویر میں دیکھ لیں





Autostart پہ کلک کریں، وہاں آپ کی ایپ کی لسٹ کھلے گی جس میں آپ دیکھ سکتے ہیں کہ کسی میں لکھا ہوگا کہ Run on startup اور کسی میں لکھا ہوگا Run on startup and Background تو آپ ان دونوں قسم کو بند کر سکتے ہیں آگے ان کو بند کرنے کا نشان دیا ہوگا۔ تو ان کو بند کر دیں۔

اگر آپ Kinguser کی ایپ Kingmaster کو ڈاونلوڈ کر دیں تو اس میں بھی یہ آپشن ہے کہ وہ ایک کلک سے سارے بیک گراونڈ کے ایپ کو عارضی طور پر بند کر دیگا جب تک دوبارہ آپ نہ کھولیں۔

اس کے علاوہ آپ کسی فائروال سافٹویئر سے بھی ان ایپ کو انٹرنیٹ استعمال کرنے کی اجازت اور منع کر سکتے ہیں۔فائروال/Firewallوالی ایپ بھی روٹ میں صرف چلتی ہیں۔

باقی اب آپ سیسٹم کے ایپ نکال سکتے ہیں اور اکثر Q Mobileمیں مسئلہ یہ ہوتاہے کہ RAMکم ہوتی ہے یاانٹرنل میموری بہت کم ہوتی ہے جس سے دوسرے ایپ انسٹال نہیں ہوپاتے،توبہتر ہے آپ Gmail, Google +,Talk, Hangouts, Email, Drive,وغیرہ جو غیر ضروری ہیں ان کو نکال دیں۔نکالنے کا طریقہ پہلے بتاچکاہوں کہ Es File Explorerسے کیسے نکال سکتے ہیں،لیکن خیال کرلیں Google Play Store, Google Servicesکو نکالنے کے بعد دوبارہ اگرانسٹال کریں تونہیں چلتے۔اور آپ Kinguserسے بھی سیسٹم کے ایپ نکال سکتے ہیں مگر اس میں سب کو نکالنے کا آپشن نہیں ہے۔

ج:روٹ والے موبائل میں گوگل پلے اسٹور وغیرہ(سیسٹم کے سافٹویئر)کو نکالنے کا طریقہ:

روٹ والے موبائل میں سیسٹم کے ایپس شروع سے ڈالے ہی نہیں،اگرڈال چکے ہوں تو Es File Explorerسے ان کو نکال سکتے ہیں۔

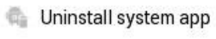
Es File Explorerکالنک:

http://www.1mobile.com/es-file-explorer-file-manager-70957.html

یا

https://play.google.com/store/apps/details?id=com.estrongs.android.pop

طریقہ یہ ہے Es File Explorerکو کھولیں۔اس نشان پہ کلک کریں۔

پھر اس پہ کلک 

کریں،پھر اس پہ کلک کرکہ

جو سافٹویئر آپ uninstallکرناچاہتے ہیں اس کو سلکٹ کرکہ اَن انسٹال کرلیں۔

گوگل پلے اسٹور کا متبادل:

اگرآپ روٹ کرنے کے بعد Google PlaystoreکوUninstall کرلیں تو اس کا متبادل یہ ہے جہاں سے آپ Appsڈاونلوڈ کرسکتے ہیں۔

http://market.1mobile.com

اس لنک پہ جا کر ڈاونلوڈ کے بٹن پہ کلک کریں،اور انسٹال کریں۔

یہ اس کا بہتر متبادل تو نہیں مگر مجبوری میں گزارا کریگا۔ گوگل کے اکاونٹ سے جتنا بچا جائے اتنا بہتر ہے کیونکہ اس کا کام تو اب یہی ہے کہ اپنے صارفیں کی مکمل معلومات حاصل کرنا۔

اور بہت سے لوگ گوگل پلے اسٹور کا متبادل FDroid کا مشورہ دیتے ہیں مگر وہ بے فائدہ ہے اس میں ۰ افیصد بھی سافٹویر نہیں ہیں۔

نوٹ: گوگل پلے اسٹور کے علاوہ دوسرے جگہوں سے موبائل ایپ ڈاونلوڈ کرنا خطرے سے خالی نہیں، خطرے سے میری مراد یہ ہے کہ اس میں جاسوسی سافٹویر کا آنا ممکن ہے، چاہے وہ موبائل مارکیٹ ہی کیوں نہ ہو، سب سے معتبر ذریعہ گوگل پلے اسٹور ہے جس میں ایپس بقاعدہ چیک ہونے کے بعد اپ لوڈ ہوتے ہیں۔

BBM چلانے اور فرینڈ ایڈ کرنے کا طریقہ

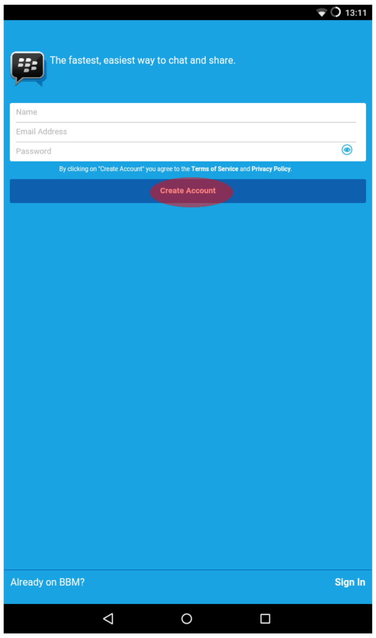
ڈاؤنلوڈ لنک:

http://www.1mobile.com/bbm-1125780.html

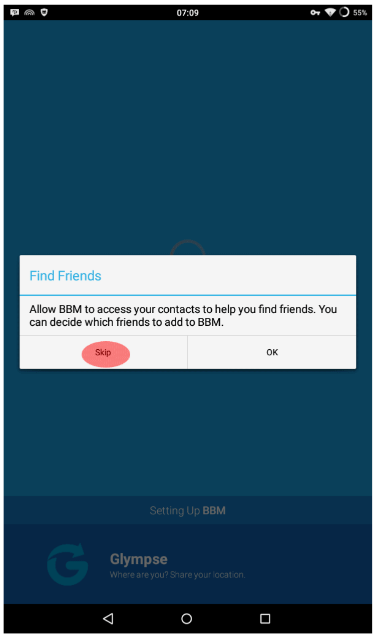
یا

https://play.google.com/store/apps/details?id=com.bbm

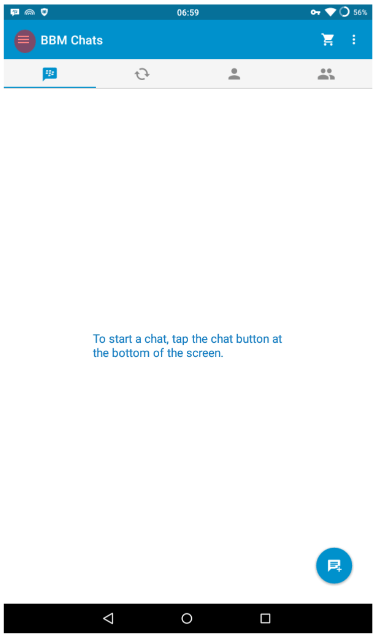
1



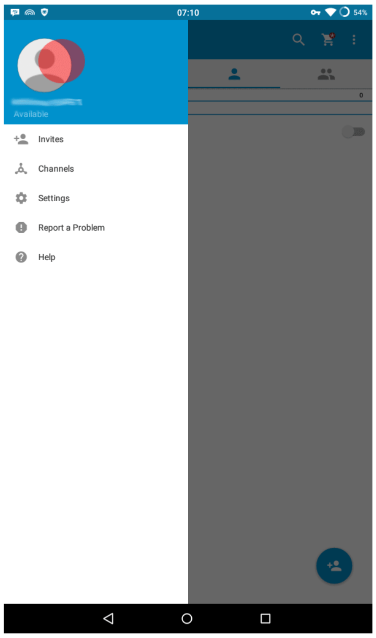
2



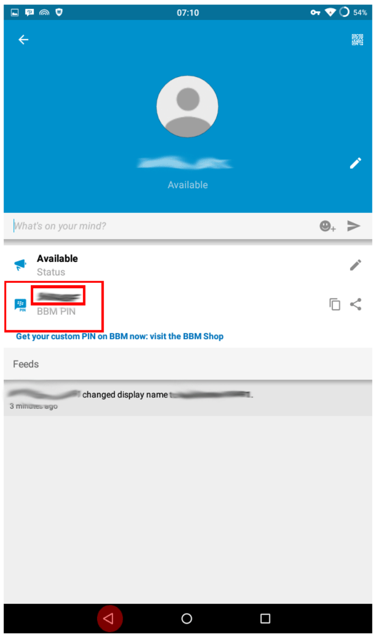
3



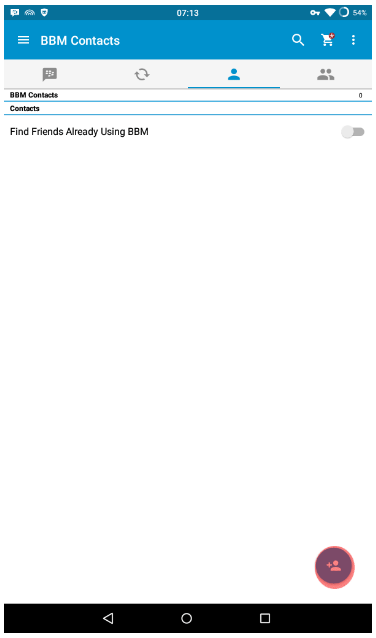
4



5



6



جیسا تصویر میں دکھایا ہے ویسا کریں، یعنی شروع میں اکاونٹ بنائیں۔ اکاونٹ آپ کسی بھی ای میل ایڈریس سے بنا سکتے ہیں جس کو آپ ویریفائی کر سکیں۔

تصویر کے نمبر کے حساب سے نکات کے نمبر :

۱۔ پہلے خانے میں وہ نام لکھیں جو آپ BBM میں استعمال کرنا چاہتے ہیں، نام ایسا رکھیں جو مشکوک نہ ہو۔ دوسرے خانے میں ای میل اور تیسرے میں پاس ورڈ

ای میل ایڈریس دینے کے بعد اپنا میل چیک کریں ایک لنک دیا ہو گا ویریفائی کیلئے اسے کلک کریں۔

۲۔ جب آپ BBM میں سائن اِن ہونگے ایک فائنڈ فرینڈ اسکرین آئے گا اسے اِسکپ کریں۔

۳۔ پھر تین لکیروں والے آپشن کو کلک کریں، جیسا تصویر ۳ میں دکھایا ہے۔

۴۔ پھر اپنے نام کے اوپر اپنے پروفائل پکچر کی جگہ کلک کریں۔

۵۔ تصویر نمبر ۵ میں آپ دیکھ سکتے ہیں کہ پھر وہاں ایک BBM پِن نمبر ہوگا، یہ آپ کا پِن نمبر ہے جس کو آپ دوسروں کو دینگے فرینڈ بنانے کے لئے، یہاں سے آپ بیک پہ جائیں۔

۶۔ تصویر ۶ میں جو نشان دکھایا ہے اسے کلک کریں یعنی ایڈ اے فرینڈ پر۔

۷۔ پھر اس نشان پہ کلک کریں

اور بھی آپشن ہونگے مگر محفوظ طریقہ یہی ہے فرینڈ ایڈ کرنے کا، اس کو کلک کرنے کے بعد اپنے دوست کا پِن نمبر داخل کریں، اس کے پاس انوائٹیشن جائیگا جب وہ اسے قبول کرلے تو آپ اس سے بات کر سکتے ہیں۔

BBM کو بند کرنے کا طریقہ: BBM میں ایک بڑی مصیبت یہ ہے کہ ہمیشہ چل رہا ہوتا ہے، اس کے سیٹنگز کو تبدیل کرنا ہوگا۔
تصویر نمبر ۴ میں دیکھیں جہاں سیٹنگز لکھا ہے وہاں کلک کریں، پھر BBM Connected Icon کے صحیح کے نشان کو ختم کریں۔

BBM میں لاگ آوٹ کرنے کا طریقہ: BBM میں لاگ آوٹ کا کوئی آپشن نہیں ہے، اس لئے اگر آپ کو BBM لاگ آوٹ کرنا ہو تو آپ اپنے موبائل کے سیٹنگز میں جائیں۔

پھر Apps/App Manager پہ کلک کریں پھر وہاں BBM کو تلاش کریں اور اس پہ کلک کریں پھر Clear Data پہ کلک کریں، اس سے BBM بالکل نیا ہو جائیگا، اور آپ لاگ آوٹ ہو جائینگے۔

BBM کا چناو کیوں؟: اینڈرائڈ میں بہت سے سافٹویر ایسے ہیں جو کہتے ہیں کہ وہ End to End Encrypted میسج بھیجتے ہیں یعنی وہ کوڈنگ کے ذریعے میسج بھیجتے ہیں جس کا بھیجنے والے اور جس کو پہنچ رہا ہے، ان دونوں کے علاوہ کسی کو معلوم نہیں ہو سکتا کہ کیا بھیج رہا ہے، یعنی اگر کوئی آپ کے نیٹ کی جاسوسی کر رہا ہے تو اس کو معلوم نہیں ہو سکتا آپ کہ کیا بھیج رہے ہو۔ مگر اکثر سافٹویر میں یہ بات غلط ثابت ہوئی ہے، خاص طور پر whatsapp پہ کہ اکثر ہیکرز نے ان کے میسج ٹریس کئے ہیں، اس لئے اب ان پہ بھروسہ نہیں کیا جاسکتا۔ مگر BBM کا ہیکرز نے تصدیق کی ہے کہ ان کے میسج کوڈنگ کے ذریعے ہوتے ہیں جس کا تیسرے بندے کو پتا نہیں چلتا کہ کیا بھیج رہے ہیں۔ البتہ ایک رپورٹ کے مطابق امریکہ کے CIA نے اب ان کے میسج کو ڈی کرپٹ کیا ہے یعنی کر سکتے ہیں۔ مگر پاکستان میں ان شاءاللہ کوئی معلوم نہیں کر سکے گا۔ اسی وجہ سے پاکستان کی حکومت نے کچھ دنوں قبل بلیک بیری کے سروس معطل کرنے کا بل منظور کرنا چاہا، جس میں BBM بھی شامل تھا، تو اس لئے ممکن ہے کہ اب پاکستان میں BBM نہ چلے اس کے لئے آپ کو پراکسی استعمال کرنا ہوگا، جس کا پچھلے ٹوریل میں بتا چکا ہوں۔

فیس بک پر انکرپٹڈ میسیج بھیجنے کا طریقہ

یہ صرف ان لوگوں کیلئے ہے جو انتہائی اہم بات کر رہے ہوں اور اس بات کو ایجینسیوں سے چھپانا چاہتے ہوں، باقی عام معلومات اور عام رابطے کیلئے اس کو استعمال نہ کریں، اگر معلومات تھوڑی اہم بھی ہو تو BBM کا استعمال کریں۔ کیونکہ اس طریقے کو استعمال کرنے سے آپ مشکوک ہونگے اور فیسبوک کی نگرانی میں آئینگے چونکہ فیسبوک پہ اب لوگوں کی تعداد کروڑوں تک جا پہنچی ہے اور ان سب کی نگرانی فیسبوک والوں کیلئے ممکن نہیں لیکن اگر آپ انکرپٹڈ میسیج بھیجینگے تو آپ لاکھوں میں ایک ہونگے اور ان کی نگرانی آسان ہوگی جو انکرپٹڈ میسیج بھیج رہے ہوں کیونکہ وہ کوڈ ہوتے ہیں، یعنی آپ کی بات کا تو نہیں پتا نہیں چلے گا مگر آپ ان کی نگرانی میں ضرور آئینگے۔

ویسے عام طور پر فیسبوک پر جب بھی اکاونٹ بنائیں تو ایسا نام رکھیں جو مشکوک نہ ہو اور ایسا تصویر لگائیں جو مجاہدین سے تعلق نہ رکھتے ہوں اگر آپ چاہتے ہیں کہ آپ کو کوئی ٹریس نہ کرے۔

ویسے تو BBM خود ہی انکرپٹڈ میسج بھیجتی ہے، مگر اگر آپ کو اس کے انکرپٹ کرنے پہ شک ہو تو بہتر ہے خود ہی انکرپٹ کریں۔

فیسبوک پہ انکرپٹڈ میسج بھیجنے کے لئے ہم Chatsecure کا استعمال کرینگے۔

ChatSecure کا مختصر تعارف: ChatSecure ایپ کو The guardian project نامی کمپنی بنا رہی ہے جو TOR کا موبائل ورشن Orbot اور Orweb بنا چکی ہے یعنی وہ TOR والے کمپنی سے منسلک ہیں۔اور TOR تو آپ کو معلوم ہوگا کہ سب سے محفوظ پراکسی فراہم کرتا ہے کمپیوٹر پر۔اس لئے ہم ان پر تھوڑا بھروسہ کر سکتے ہیں کہ ان کی سیکیورٹی اچھی ہوگی۔ ChatSecure کا پرانا نام Gibberbot ہے۔

چیٹ سیکیور کا ڈاونلوڈ لنک:

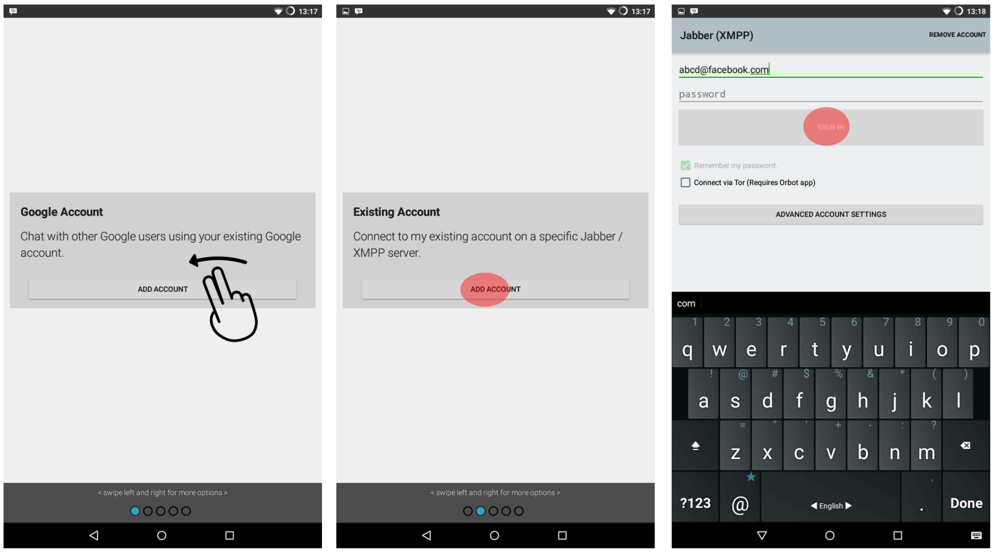
https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im

یا

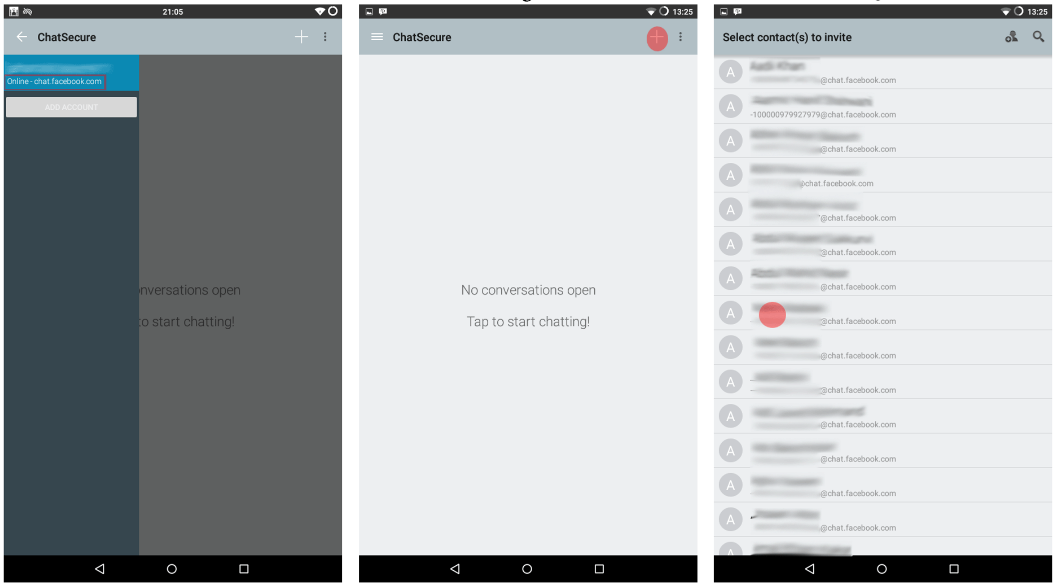
http://www.1mobile.com/chatsecure-124348.html

اب آپ ان تصویروں کو ملاحظہ فرمائیں۔

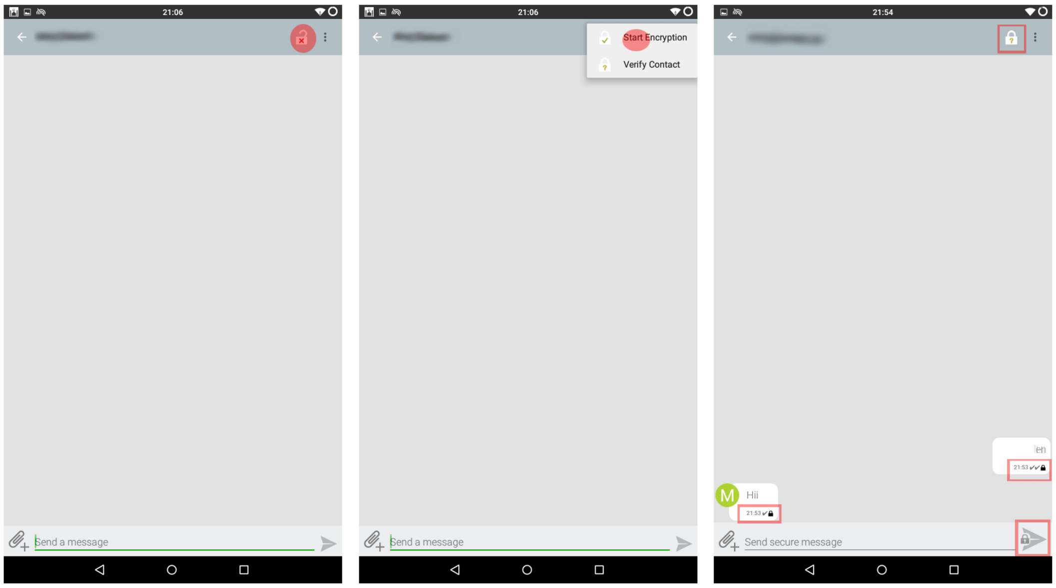
1 2 3



4 5 6



7 8 9



تصویر کے لحاظ سے نکات کے نمبر

۱۔پہلے اسکرین پہ آپ کو گوگل اکاونٹ نظر آئیگا، آپ گوگل کا آکاونٹ بھی استعمال کر سکتے ہیں، مگر فی الحال آپ کو فیسبوک کا صرف بتانا ہے، تو آپ اس کو سائیڈ پہ کریں، یعنی سوائپ کریں اور دوسرا اسکرین لائیں۔

۲۔دوسرے اسکرین میں Existing Account لکھا ہوگا اس میں Add Account پہ کلک کریں۔

۳۔تیسرے تصویر میں جیسے دکھایا ہے کہ اپنا فیسبوک کی ای میل/آئی ڈی اور فیسبوک ہی کا پاسورڈ ڈالیں اور سائن ان کریں۔ فیسبوک آئی ڈی وہ ہے جیسے آپ اپنا پروفائل کھولتے ہیں تو نظر آتا ہے اور اگر آپ نے ابھی تک نہیں بنائی ہوئی ہے تو ایک نمبر آئیگا مثلاً آپ کا پروفائل پہ نام اگر ایسا ہے https://m.facebook.com/mim48 تو آپ

یہاں آئی ڈی پہ mim48@facebook.com لکھینگے، اگرنام نہیں آرہا تو جو آئی ڈی نمبر نظر آئے وہی لکھ دیں ،اس طرح 8876767767656569@facebook.com .

۴۔سائن ان ہونے کے بعد آپ انتظار کریں تا کہ آن لائن لکھا نظر آئے جیسے تصویر ۴ میں دکھایا ہے۔

۵۔پھر + کے نشان پہ کلک کریں

۶۔پھر آپ کے کنٹیکٹس کی لسٹ کھلے گی، یہاں سے آپ جس سے بات کرنا چاہتے ہیں، اس کو کلک کریں۔

نوٹ: صرف ان لوگوں سے انکرپٹڈ میسج کر سکتے ہیں جو چیٹ سیکیور استعمال کر رہے ہوں، یعنی دونوں کے پاس انسٹال ہونا ضروری ہے، وگرنہ عام چیٹ ہو گی

۷۔پھر تالا کے نشان پہ کلک کریں۔

۸۔اور start encryption پہ کلک کریں۔

۹۔پھر آپ میسیج بھیجیں اور دیکھیں کہ واقعی انکرپٹڈ ہے، اس کیلئے دیکھیں کہ تالوں کا نشان بند ہو، جیسے تصویر ۹ میں دکھایا ہے سرخ خانوں میں۔

اگر آپ جس سے بات کرنا چاہتے ہو اس کے پاس یہ انسٹال نہیں ہو اور آپ start encryption جب کرینگے تو اس کے پاس ایک ریکوسٹ آئیگی کہ چیٹ سیکیور انسٹال کر لیں۔

اس کے بعد یہ چیک کرنے کے لئے کہ واقعی انکرپٹڈ ہیں تو آپ اپنا فیسبوک اکاونٹ کسی براوزر سے یا فیسبوک میسینجر سے دیکھ لیں اور میسیجز چیک کر لیں، کوڈ میں لکھے ہیں یا نہیں۔

اگر کوڈ میں لکھے ہوں تو سمجھ لیں ٹھیک چل رہا ہے اگر کوڈ نہ ہو تو کام نہیں کر رہا۔

اس کو سیٹ کرنے میں کوئی بھی مسئلہ پیش آرہا ہو تو آپ ہم سے رابطہ کر کہ پوچھ سکتے ہیں، اور اسی پوائنٹ کا نمبر بتائیں جو آپ کو سمجھ نہیں آرہا یا مسئلہ پیش آرہا ہے۔

چیٹ سیکیور میں آپ اس کے اپنے سرور سے بھی اکاونٹ بنا سکتے ہیں، جو فیس بک سے زیادہ بہتر ہو گا

اُربوٹ / Orbotاستعمال کرنے کا طریقہ

جیسا کہ پہلے بتا چکا ہوں کہ Tor کے موبائل ورشن کا نام اُربوٹ ہے یعنی اپنے آئی پی ایڈریس کو چھپانے کیلئے استعمال ہوتا ہے۔اس کے سارے فنکشن صرف روٹ والے موبائل میں ہی چلتے ہیں ویسے بغیر روٹ میں صرف براوزنگ کر سکتے ہیں وہ بھی Orweb یا Orfox کو ساتھ انسٹال کر کہ اس لئے پہلے اس کا متبادل F Secure Freedome کا بتایا تھا مگر جن کے موبائل روٹ کئے ہوئے ہیں وہ یہی استعمال کریں۔کیونکہ یہ کئی وجوہات کی بناپر اس سے بہتر ہے اور مفت بھی ہے،اس کی سیکیورٹی Freedome سے کافی بہتر ہے۔

اس کو یہاں سے ڈاونلوڈ کرکہ انسٹال کریں:

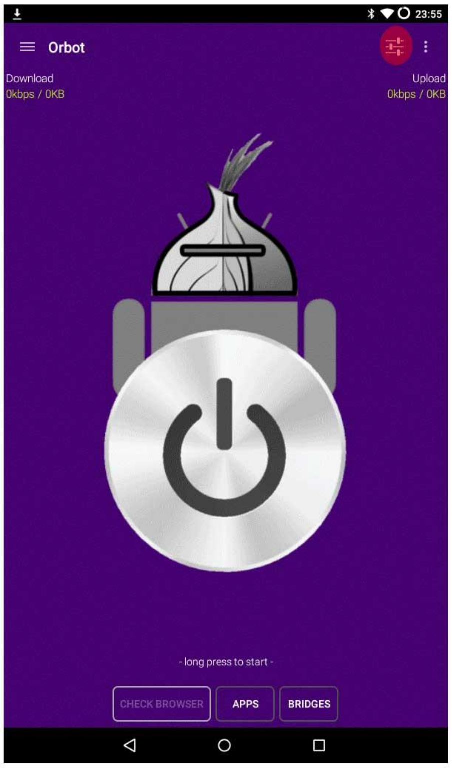
http://www.1mobile.com/orbot-proxy-with-tor-124394.html

یا

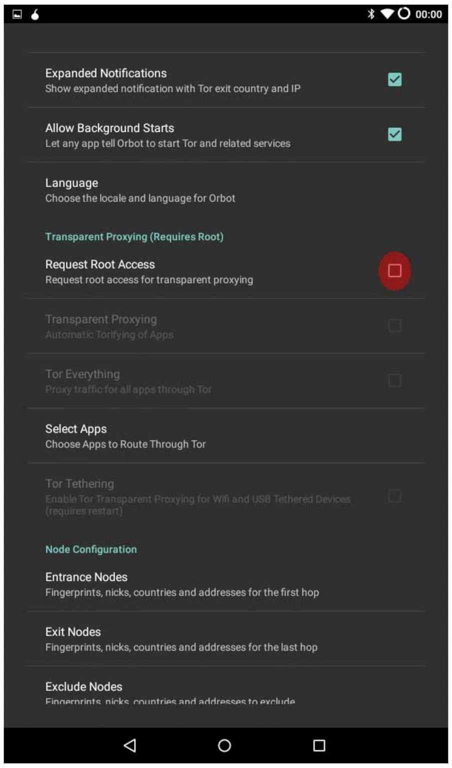
https://play.google.com/store/apps/details?id=org.torproject.android

پھر جیسا تصویر میں دکھایا ہے ویسا کریں

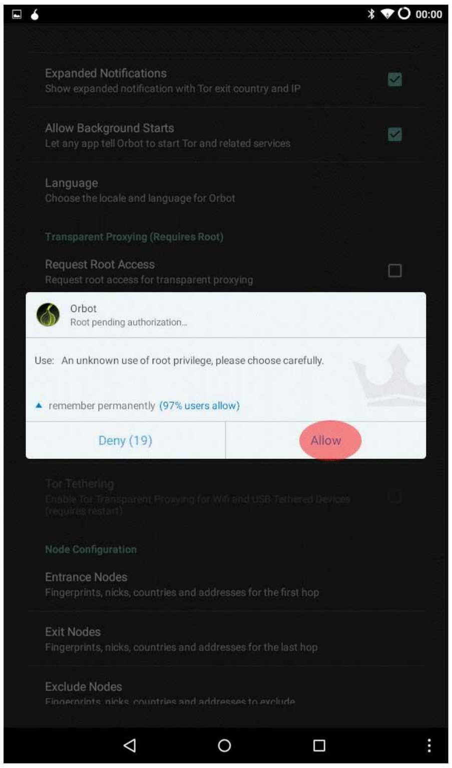
1



2



3

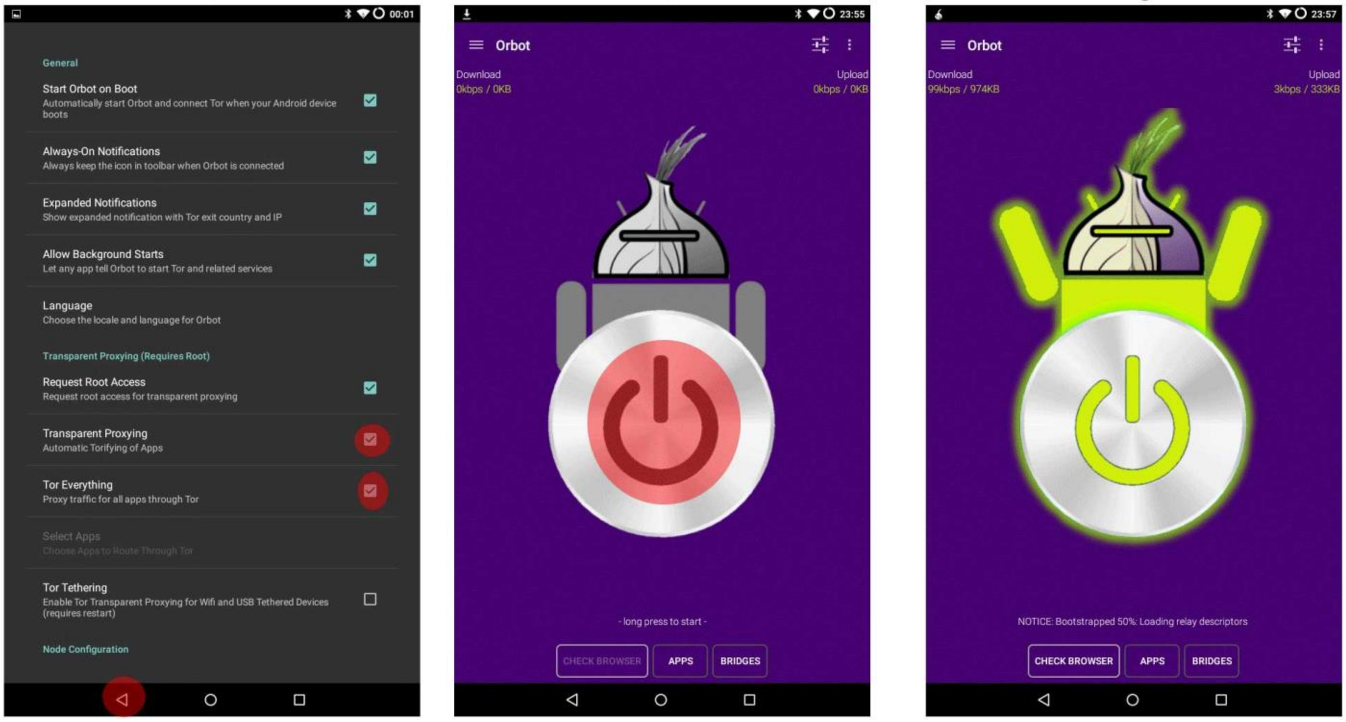


۱۔سب سے پہلے سیٹنگز میں جائیں۔

۲۔ Transparent Proxying کے خانے میں Request Root Access پہ صحیح کا نشان لگائیں۔

۳۔چونکہ یہ روٹ کا پرمیشن چاہتا ہے اس لئے یہاں کلک کرنے کے بعد وہ روٹ ایکسس چاہے گا اسے Allow کر دیں۔

4 5 6



۴۔ پھر اسی سیٹنگز میں Transparent Proxying اور Tor Everything کو بھی صحیح کا نشان لگائیں۔ اس سے اب آپ کی مکمل انٹرنیٹ ٹریفک ٹور سے ہی چلے گی۔ یہاں اب بیک پہ جائیں۔

۵۔ پھر پاور / On کے بٹن کو ۵ سے ۱۰ سیکنڈ دبائیں یہاں تک کہ وہ روشن ہو اور ایپ آن ہو جائے۔

اب یہ دیکھنے کیلئے کہ واقعی آئی پی ایڈریس تبدیل ہو گیا ہے اور انٹرنیٹ ٹور سے ہی چل رہا ہے، اس کیلئے Check Browser پہ کلک کریں اور کوئی سا براوزر سلکٹ کریں۔ وہاں لکھا آئیگا کہ

Your browser is configured to tor۔

اس کے علاوہ بھی آپ چیک کر سکتے ہیں کوئی سا بھی براوزر کھولیں اور اس میں

whatismyipaddress.com

پہ جائیں دیکھیں کہ اصل ائی پی ایڈریس ظاہر ہو رہا ہے یا دوسرا۔

نوٹ: ٹور سے آپ اپنی مرضی کے ملک کے آئی پی استعمال نہیں کر سکتے۔ ہر دفعہ دوسرے ملک کا آئی پی ہو گا۔
اس کے براوزر یعنی Orfox اور Orweb کی سیکیورٹی باقی براوزر سے کافی اچھی ہے اور وہ webrtc کا مسئلہ بھی ان میں حل کیا ہوا ہے۔

پہلے Orweb کے نام سے براوزر تھااب Orfox متعارف کروایاہے مگر Orfox فی الحال ٹیسٹ ورشن ہے ابھی تک اس کا اصل اور متوازی ورشن نہیں آیا۔
مگر ان دونوں براوزر کے فنکشن باقی براوزر سے کم ہیں۔

جن کے موبائل روٹ نہیں ہیں وہ اس اُربوٹ کو Orweb یا Orfox کے ساتھ ہی استعمال کر سکتے ہیں اور صرف براوزنگ ہی کر سکتے ہیں۔

Orfox کا ڈاونلوڈ لنک: http://www.apkmirror.com/apk/the-guardian-project/orfox/orfox-38-0-android-apk-download

Orweb کا ڈاونلوڈ لنک: http://www.1mobile.com/orweb-private-web-browser-133606.html

یا

https://play.google.com/store/apps/details?id=info.guardianproject.browser

ٹیلی گرام میسینجر / Telegram کا استعمال

جیسا پہلے بتا چکا ہوں کہ بعض ایپ ایسے ہیں جو کہتے ہیں کہ وہ End to End Encrypted میسج بھیجتے ہیں ان میں سے ایک ٹیلی گرام بھی ہے۔یعنی کوڈ میں اپنے میسج بھیجتے ہیں۔یہ whatsapp کے مقابلے میں زیادہ بہتر اور زیادہ محفوظ ہے۔اور استعمال کا طریقہ بھی whatsapp جیسا ہی ہے۔تو بہتر ہے کہ whatsapp کی جگہ اسی کو استعمال کریں،اگرچہ اس پر بھی مکمل بھروسہ نہیں کر سکتے کہ واقعی کوڈ میں میسج بھیجتا ہے یا نہیں مگر whatsapp سے کافی بہتر ہے۔آپ اسے یہاں سے ڈاونلوڈ کر کہ انسٹال کریں۔

http://www.1mobile.com/telegram-1013814.html

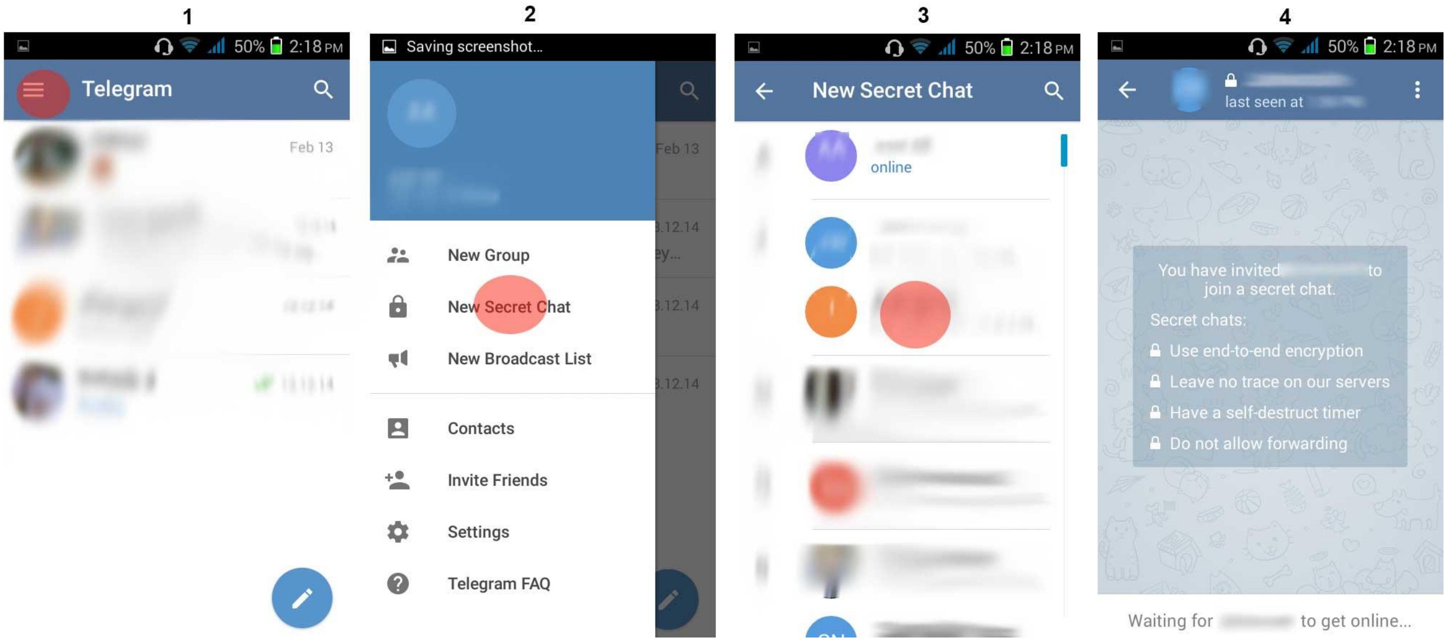
یا

https://play.google.com/store/apps/details?id=org.telegram.messenger

چلانے کا طریقہ بالکل whatsapp جیسا ہے،شروع میں اپنا نمبر ڈالیں ایک کوڈ آئیگا اگر وہ نمبر دوسرے موبائل میں ہو اگر اسی موبائل میں ہو تو خود باخود اکاونٹ بن جائیگا۔اور آپ کے جو کنٹیکس فون میں موجود ہیں جو یہ استعمال کرتے ہوں ان کی لسٹ آ جائیگی۔

اس میں مزید محفوظ طریقے سے بات کرنے کے لئے Secret Chat کا استعمال کریں،اس کا طریقہ یہ ہے۔

جیسا تصویر میں دکھایا ہے



۱۔ڈراپ مینیو / تین لکیر والے آپشن کو کلک کریں

۲۔ News Secret Chat کو کلک کریں

۳۔کسی بھی کنٹیکٹ کو کلک کر کہ چیٹ کر لیں۔

روٹ والے موبائل میں IMEI نمبر تبدیل کرنے طریقہ

یہ بات تو سبھی کو پتا ہے کہ آجکل IMEI نمبر بھی ٹریس ہوتے ہیں جس سے اگر ایک ہی موبائل سے کئی سم لگائیں تو تب بھی پتا چلے گا کہ یہ ایک ہی بندہ ہے اور ایک ہی موبائل ہے۔ تو اس IMEI نمبر تبدیل کرنے کے بہت سے فوائد ہیں۔

نوٹ: اس کی ہم گارنٹی نہیں دیتے کہ پھر موبائل دوبارہ صحیح کام کریگا۔ اور اپنا IMEI نمبر لکھ کر کہیں محفوظ بھی کرلیں تاکہ دوبارہ اس کو صحیح کر سکیں۔

بغیر روٹ والے بھی اس کو آزمالیں شاید کام کرے۔

اپنے موبائل کا IMEI نمبر دیکھنے کیلئے اپنے موبائل پر *#06# ڈائل کریں

IMEI نمبر تبدیل کرنے کیلئے ہمیں Engineer Mode میں جانا پڑیگا۔ اس کا طریقہ یہ ہے کہ اپنے موبائل میں یہ نمبر ڈائل کریں:

##3646633#*#*

یا

*#7465625#

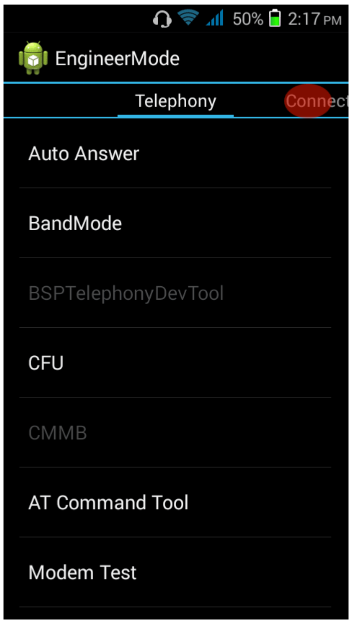
ان میں سے کوئی ایک نمبر ڈائل کریں تو موبائل کا Engineer Mode کھل جائیگا۔

اگر ان دونوں سے بھی Engineer Mode نہ کھلے تو آپ یہ ایپ ڈاونلوڈ کرکہ انسٹال کر کہ چلائیں۔

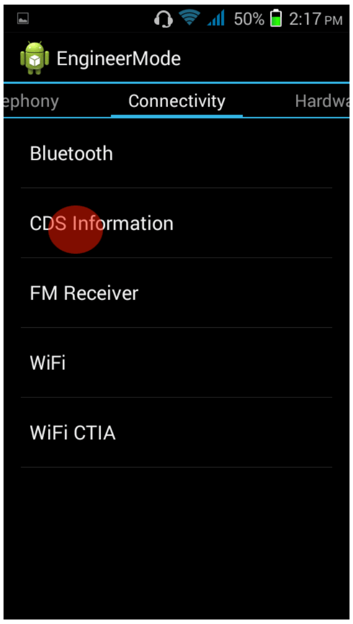
https://play.google.com/store/apps/details?id=com.Go.EngModeMtkShortcut&hl=en

اس سے تقریباً Engineer Mode آجائیگا۔ پھر ایسا کریں جیسا تصویر میں دکھایا ہے۔

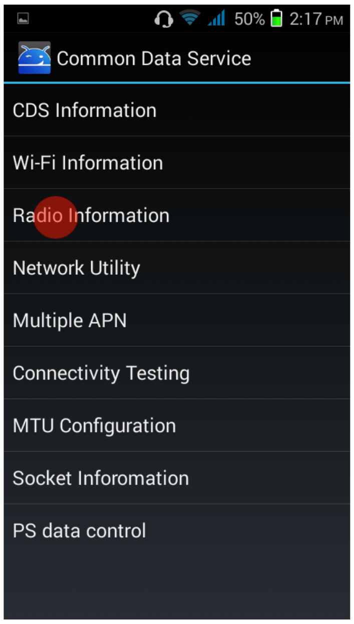
1



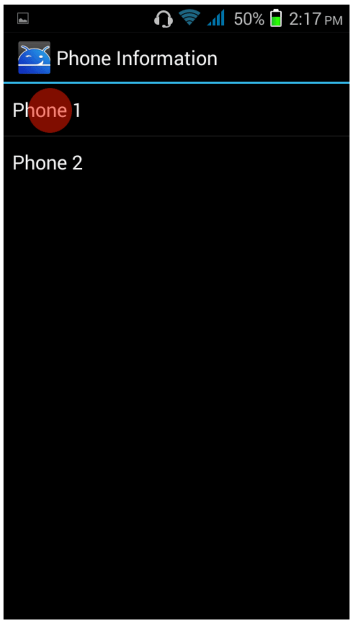
2



3



4



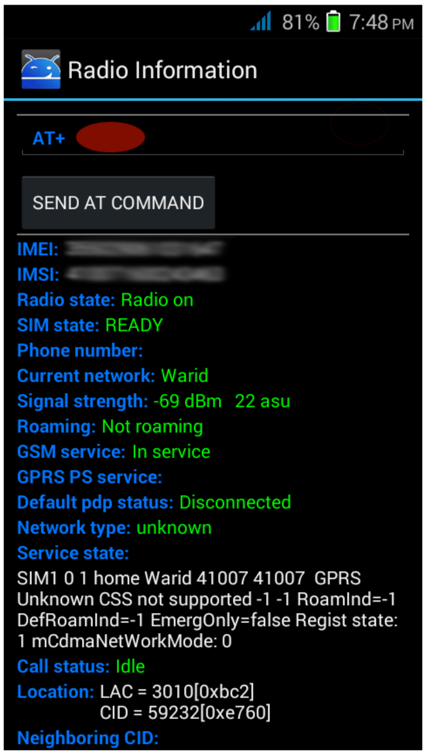
۱۔پہلے Connectivity میں جائیں۔

۲۔پھر CDS information میں جائیں۔

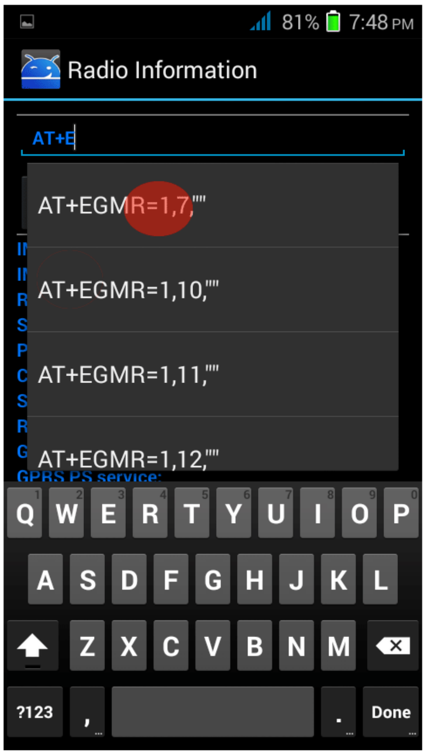
۳۔پھر Radio Informationمیں جائیں۔

۴۔پھر جس سم کی IMEI نمبر تبدیل کرنا ہو اس کو کلک کریں۔

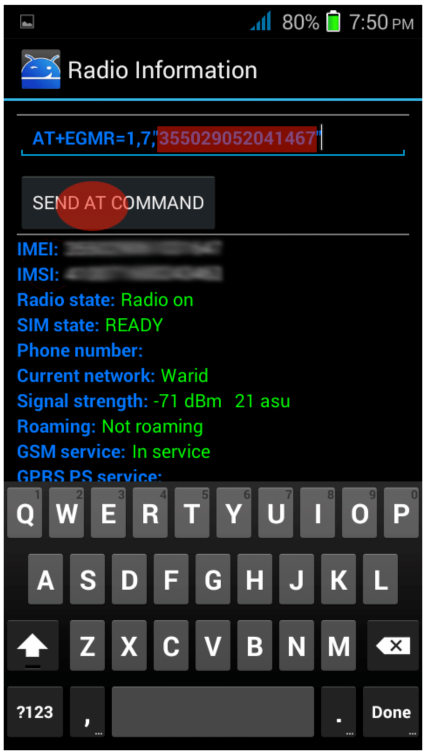
5



6



7



۵۔پھر اب AT+ کے سامنے کلک کریں۔

۶۔اور اس کے سامنے ایک کوڈ لکھا ہوگا، آپ E لکھیں خود ہی آپ آپشن آجائنگے آپ اگر سم اول کا IMEI نمبر تبدیل کر رہے ہیں تو آپ ""AT+EGMR=1,7 کو کلک کریں اور اگر سم دوم کو سیٹ کر رہے ہوں تو ""AT+EGMR=1,10 کو کلک کریں۔

۷۔ان "" کے درمیان اپنا مطلوبہ IMEI نمبر لکھیں جو آپ ظاہر کرنا چاہتے ہیں۔جو تصویر میں سرخ خانے میں دکھایا ہے۔ IMEI نمبر 15 ہندسوں کا ہونا چاہئے۔اب مکمل کوڈ کچھ اس طرح ہوگی:

AT+EGMR=1,7"355029052041467"

باقی کوڈ سب کا یہی ہے بس یہ پیلے رنگ میں جو ہے اسے بس اپنی مرضی کا دیں اور آخر میں Send At Command پہ کلک کریں۔

اب اپنا موبائل بند کر کہ دوبارہ چلائیں اور IMEI نمبر دیکھنے کیلئے #06#* ڈائل کریں اور دیکھیں کیا واقعی تبدیل ہو گیا ہے یا نہیں۔

ایک دفعہ جب تبدیل کر دیا پھر واپس اسی طریقے سے اپنا پرانا IMEI نمبر کر سکتا ہیں اس کے علاوہ کوئی اور طریقہ نہیں،ہاں موبائل کو مکمل فارمیٹ کے بعد دوبارہ وہی IMEI نمبر ہوگا۔

نوٹ: ہر موبائل میں Engineer Mode الگ طرح کا ہوتا ہے اس لئے آپ صرف ان نام کو یاد رکھیں اور ان میں جائیں چاہے جدھر ھوں

موبائل میں مزید کچھ احتیاطیں

۱۔اینٹی وائرس: موبائل میں اینٹی وائرس ضرور ڈالیں،یہ آپ کو جاسوسی سافٹویئر سے بچاتا ہے۔اور بھی کئی فیچرز ہوتے ہیں موبائل کے اینٹی وائرس میں مثلاً ہسٹری،کیش وغیرہ کلین کرنا،ایپ لاک وغیرہ۔۔

360اینٹی وائرس کا لنک:

https://play.google.com/store/apps/details?id=com.qihoo.security&hl=en

یا

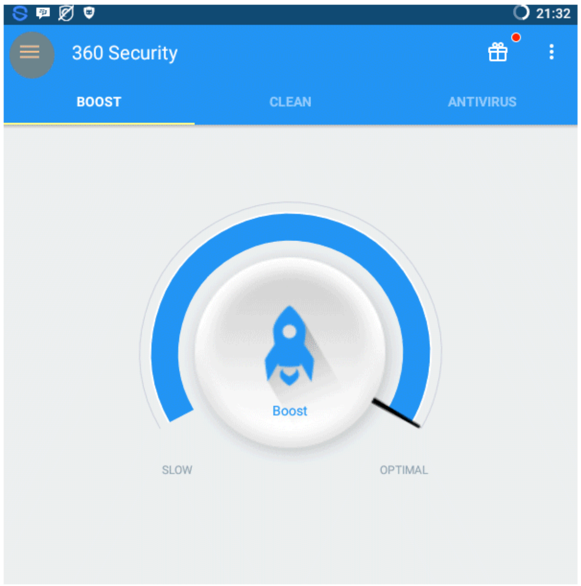
http://www.1mobile.com/360-security-antivirus-free-download-2143238-direct.html

۲۔فائروال: فائروال وہ سافٹویئر ہے جو دوسرے سافٹویئر کو چلنے سے یا انٹرنیٹ استعمال کرنے سے روکتا ہے جب تک آپ خود اس کو اجازت نہ دیں۔

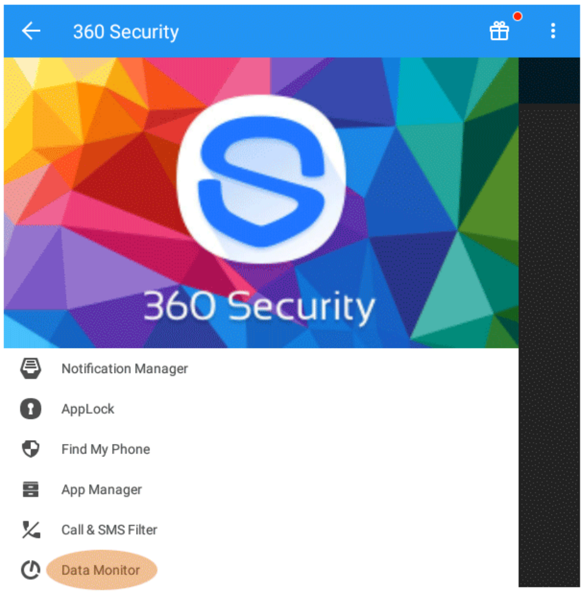
مگر یہ فائروال سافٹویئر صرف روٹ والے موبائل میں ہی چلتے ہیں۔اوپر جس اینٹی وائرس کا لنک دیا ہے اس میں فائروال بھی موجود ہے،

سب سے پہلے اینٹی وائرس کھولیں،اس میں فائروال کی سہولت حاصل کرنے کیلئے نیچے تصویر ملاحظہ فرمائیں۔

1



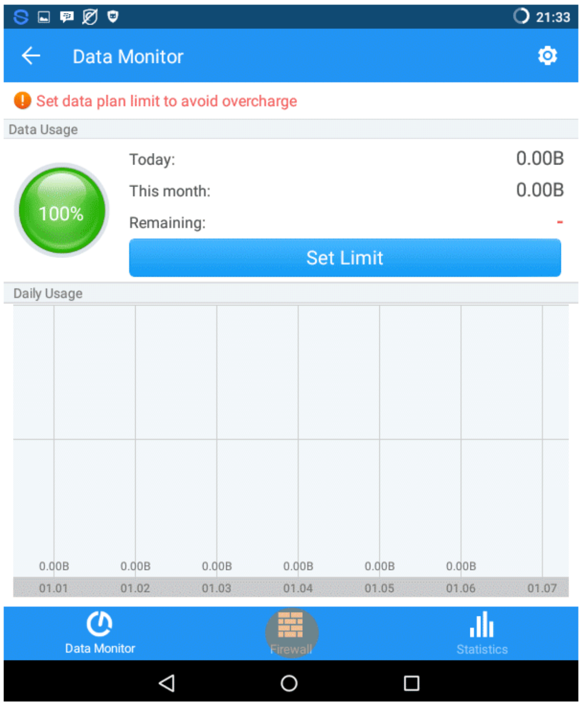
2



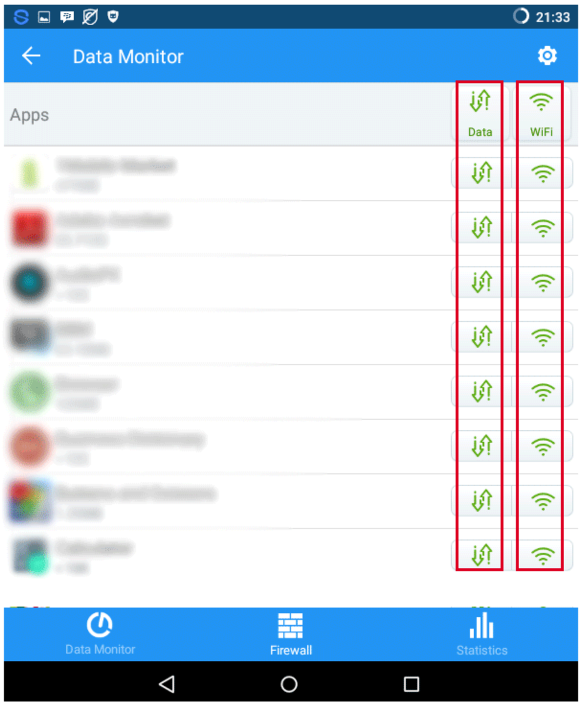
۱۔ڈراپ مینیو یعنی تین لکیروں والے آپشن کو کلک کریں۔

۲۔پھر Data Monitor کو کلک کریں۔

3



4



۳۔ Firewall پہ کلک کریں،پہلی مرتبہ کلک کرنے سے روٹ کی پرمیشن دینی ہوگی،روٹ کی پرمیشن دینے کے بعد آپ اگلے اسکرین کی طرف جائینگے۔

۴۔اب ان سافٹوئیر کی لسٹ ہوگی جو انسٹال ہیں اوران کے سامنے Data اور Wifi کا نشان ہوگا،ڈیٹا کا نشان ختم کرنے سے یہ ایپ موبائل نیٹ سے انٹرنیٹ استعمال نہیں کر سکینگے اور وائی فائی کا نشان ختم کرنے سے یہ وائی فائی کے انٹرنیٹ سے انٹرنیٹ استعمال نہیں کر سکینگے،دونوں کو ختم کرنے سے وہ ایپ انٹرنیٹ استعمال نہیں کر سکیگی جب تک آپ دوبارہ اُن کو On نہ کریں۔

اس کے علاوہ آپ Droidwall بھی استعمال کر سکتے ہیں،طریقہ یہی ہے۔

Droidwall کا لنک یہ ہے:

http://www.1mobile.com/droidwall-android-firewall-2000556.html

یا

https://play.google.com/store/apps/details?id=com.googlecode.droidwall.free

فیس بک اور ٹیلی گرام کے اکاونٹ ویریفکیشن کیلئے نمبر حاصل کرنے کا طریقہ

چونکہ اب مجاہدین کی خبریں ٹیلی گرام پر بھی آنے لگی ہیں اور اُن کے میڈیا اس پہ چل رہے ہیں تو ایسی صورت میں اپنے نمبر کے ذریعے بنائے ہوئے اکاونٹ کے ساتھ ایسے چینل / گروپ کو جوائن کرنا مناسب نہیں اس لئے یہ طریقہ استعمال کریں۔

اس کے لئے موبائل کا ہونا ضروری ہے اور اگر آپ کے پاس اینڈرائیڈ یا آئی او ایس والا موبائل نہیں اور کمپیوٹر سے کرنا چاہتے ہیں تو Bluestack یا Droid 4x یا اس جیسے دوسرے سافٹویئر ڈاونلوڈ کریں جن کے ذریعے سے آپ اینڈرائیڈ ایپ کمپیوٹر میں چلا سکتے ہیں۔

نمبر وریفائی کیلئے ہم ایک ایپ کا استعمال کرینگے جس کا نام ہے "نیکسٹ پلَس/NextPlus" یا "ٹیکسٹ پلَس/TextPlus"، یہ دونوں ایک ہی کمپنی کی ہیں اور ایک ہی ڈیٹا سینٹر ہے، یہ ایپ آپ کو ایک مستقل امریکہ کا نمبر دیتا ہے جس کے ذریعے آپ کوئی بھی اکاونٹ بنا سکتے ہیں، سوائے واٹس ایپ کے۔

اس کے زیادہ استعمال کی وجہ سے آج کل نیکسٹ پلس پہ آسانی سے نمبر نہیں مل رہا مگر ٹیکسٹ پلس پہ نمبر مل جاتا ہیں، اس لئے ہم پہلے ٹیکسٹ پلس کا بتائینگے اور پھر نیکسٹ پلس کا۔

سب سے پہلے آپ اس ایپ کو ڈاونلوڈ کریں یہاں سے:

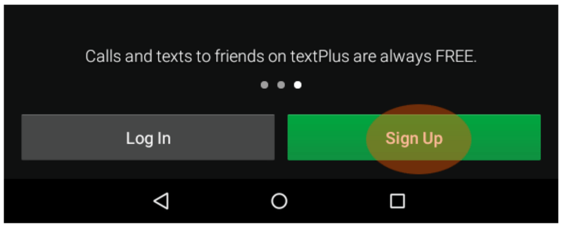
www.1mobile.com/textplus-free-text-calls-13881.html

یا

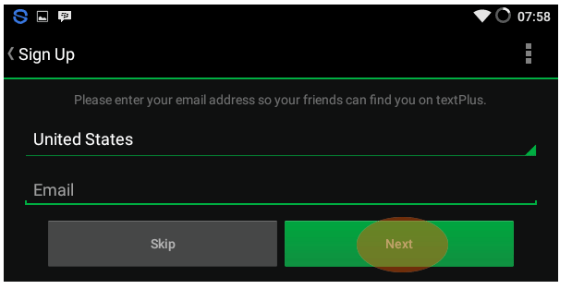
https://play.google.com/store/apps/details?id=com.gogii.textplus

انسٹال کرنے کے بعد اسے کھولیں، اور پھر نیچے دیئے گئے اس تصویر پہ عمل کریں۔

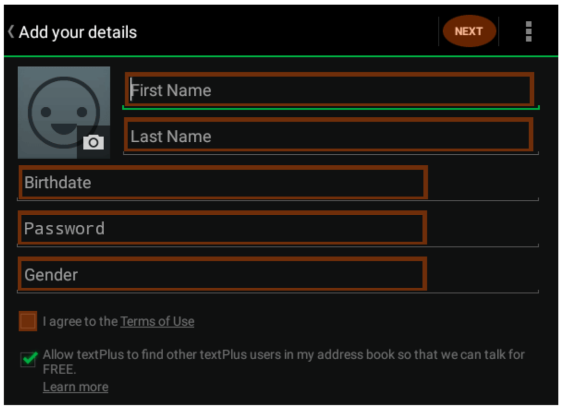
1



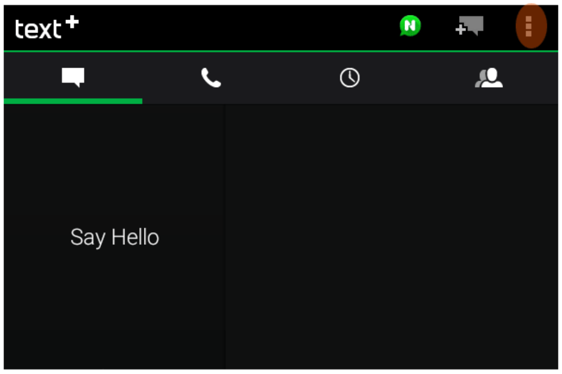
2



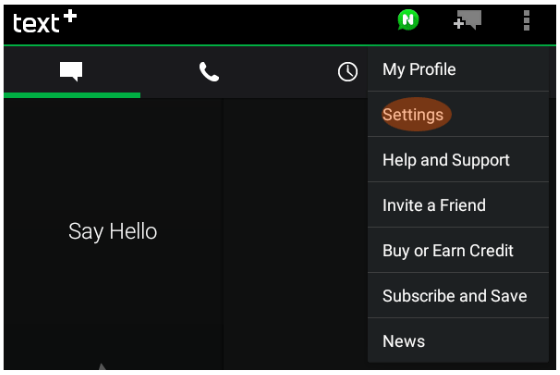
3



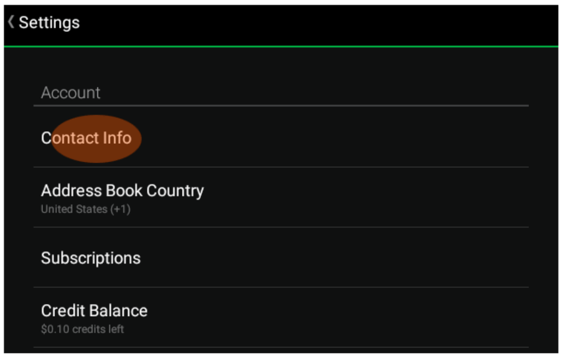
4



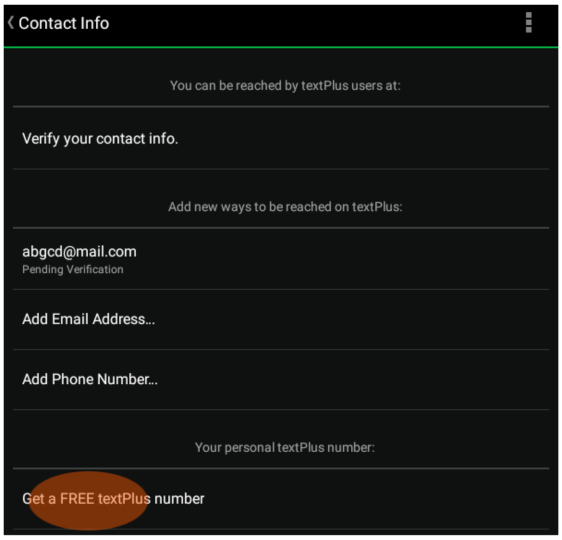
5



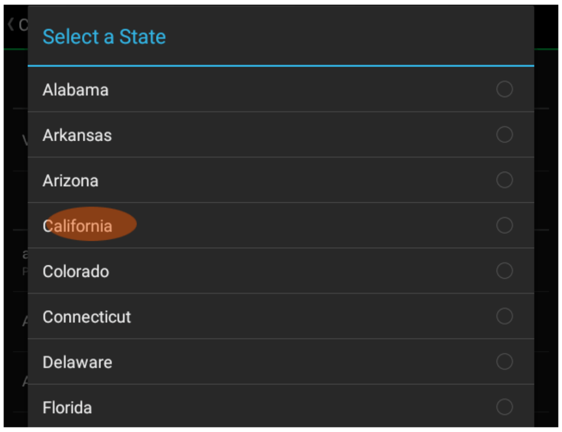
6



7



8



۱۔سائن اَپ پہ کلک کریں۔

۲۔ای میل ایڈریس دیں اور نیکسٹ پہ کلک کریں،ایسا ای میل ایڈریس جس کو آپ پھر ویری فائی کر سکیں یعنی اُس پہ ایک لنک کلک کر سکیں۔

۳۔اس فارم کو پُر کریں،اور پاسورڈ بھی یادرکھیں کیونکہ آپ کو یہ بعد میں کام آسکتا ہے۔

۴۔اب جب اکاونٹ بن گیا اب آپ اپنے ای میل کھول کہ اس پہ لنک آیا ہوگا اس پہ کلک کریں،اوراس ایپ میں اب نمبر حاصل کرنے کیلئے ڈراپ مینیو یعنی تین نکتوں والے آپشن پہ کلک کریں جیسا تصویر نمبر ۴ میں دکھایا ہے۔

۵۔پھر سیٹنگز پہ کلک کریں۔

۶۔پھر کنٹیکٹ اِنفو پہ کلک کریں۔

۷۔ Get a FreePlus number پہ کلک کریں۔

۸۔پھر امریکہ کے کسی اسٹیٹ کو سیلکٹ کریں، آپ کو نمبر مل جائیگی۔

اب اسی نمبر کے ذریعے آپ ٹیلی گرام اور فیس بک اکاونٹ بنا سکتے ہیں۔

نوٹ:

۱۔ٹیکسٹ پلس میں آج کل یہ مسئلہ پیش آرہا ہے کہ میسج نہیں آتے اور نہ وائس کال آتی ہیں، اگر یہ آپ کے ساتھ بھی ہورہا ہو تو آپ اِس کا دوسرا ایپ یعنی نیکسٹ پلس ڈاونلوڈ کر کہ انسٹال کریں۔اُس میں مسئلہ یہ تھا کہ نمبر نہیں ملتا آسانی سے، اب آپ جب ٹیکسٹ پلس میں اکاونٹ بنا کہ نمبر حاصل کر چکے تو آپ وہاں صرف لوگ اِن ہو جائیں تو یہ نمبر آپ کو وہاں بھی مل جائیگا جیسا پہلے بتا چکا ہوں دونوں ایک ہی کمپنی ہیں اور ایک ہی ڈیٹا بیس/سینٹر ہے، اب یہ نمبر آپ کے اکاونٹ کے ساتھ فیکس ہے جب بھی آپ اپنے اِس اکاونٹ کے ساتھ لوگ اِن ہونگے آپ اس نمبر کے ذریعے میسج وصول کر سکتے ہیں۔اس کا استعمال بعینہ اُسی جیسا ہے۔

اور ڈاونلوڈ یہاں سے کریں

http://www.1mobile.com/nextplus-free-sms-text-calls-download-2308046-direct.html

یا

https://play.google.com/store/apps/details?id=me.nextplus.smsfreetext.phonecalls&hl=en

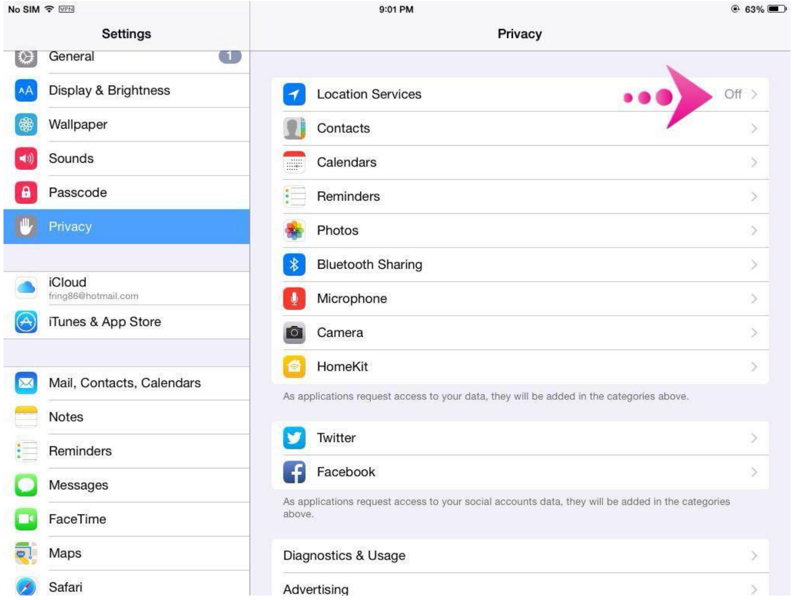
۲۔اگر آپ ٹیلی گرام کا ویریفیکیشن میسج نیکسٹ پلس پہ بھی وصول نہ کر سکیں تو کوئی مسئلہ نہیں انتظار کریں آپ کو وائس کال ضرور آئیگی ۵ منٹ میں، جس میں کوڈ بتایا ہوگا۔

اس کے علاوہ بھی آپ دوسرے ایپ بھی استعمال کر سکتے ہیں جو آپ کو امریکہ یا دوسرے ممالک کا نمبر فراہم کریں مگر کچھ عرصہ سے باقی سافٹوئیر زنے الگ سے فون نمبر دینے کی سہولت کو ختم کیا ہے مثال کے طور پر TextMe, Hushed, Burner, Talkatone, Voxofone وغیرہ۔

iOS (یعنی آئی فون اور آئی پیڈ) کی سیکیورٹی

سیٹنگز میں ایپ پرمیشن اور دیگر تبدیلیاں

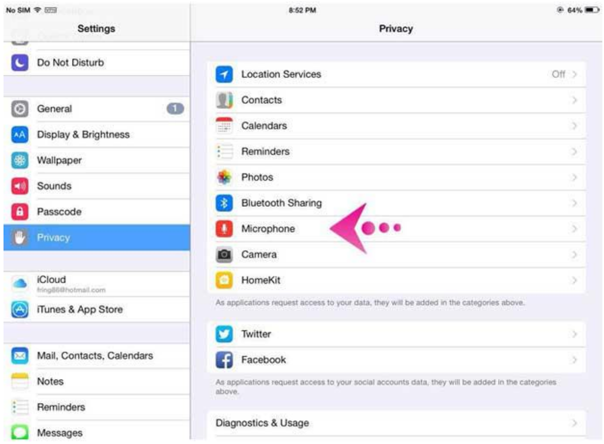
۱: لوکیشن کو بند کرنا: سب سے پہلے سیٹنگز میں جائیں، پھر Privacy پہ کلک کریں، سب سے پہلے لوکیشن کے آپشن کو بند کریں



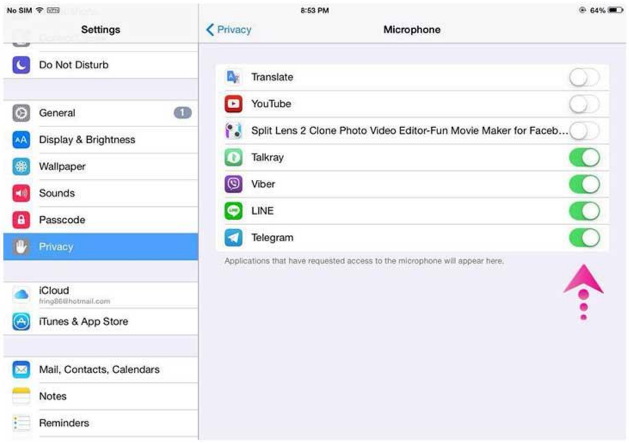
اس کے لئے لوکیشن سروس پہ کلک کر کہ اسے Off کریں۔اس سے اب کوئی ایپلیکیشن آپ کی لوکیشن بغیر آپ کی اجازت کے معلوم نہیں کریگا۔

۲۔مائکروفون اور دیگر چیزوں کی پرمیشن کو محدود کرنا: پھر اسی خانے میں Microphone پہ کلک کریں،اس کے بعد پھر ان ایپ کی فہرست کھلیگی جو مائکروفون تک رسائی حاصل کرتے ہیں،تو یہاں صرف ان ایپ کو اجازت دیں جس پہ آپ ریکارڈنگ بھیجتے ہوں،جیسے نیچے تصویر میں دکھایا ہے

1



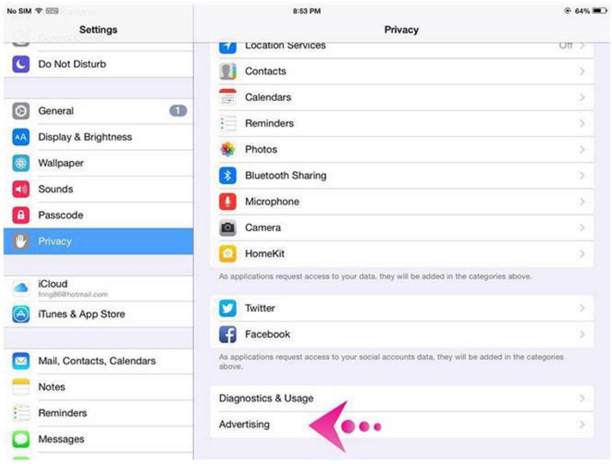
2



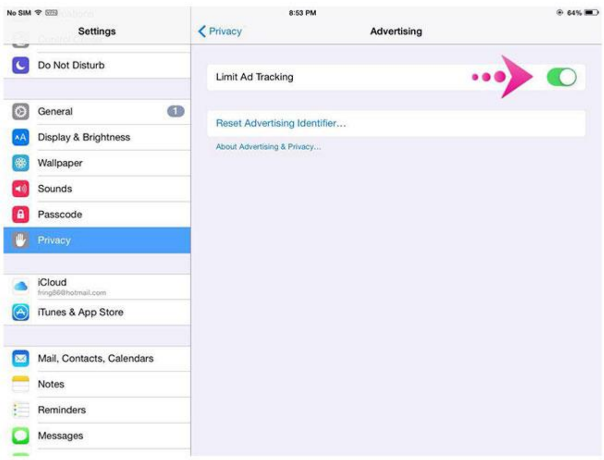
پھر اسی طرح کیمرے کے آپشن میں جائیں اور وہاں بھی یہی کریں۔اور کنٹیکٹس اور فوٹوز کو بھی اسی طرح ترتیب دیں کہ کون کون سے ایپ اس تک رسائی حاصل کر سکتے ہیں۔

۳۔ایڈز/اشتہارات کو محدود کرنا: پھر اسی پرائیویسی خانے میں نیچے دیکھیں Advertising لکھا ہوگا اس پہ کلک کریں،اور اس میں Limit ad tracking کو On کریں

1

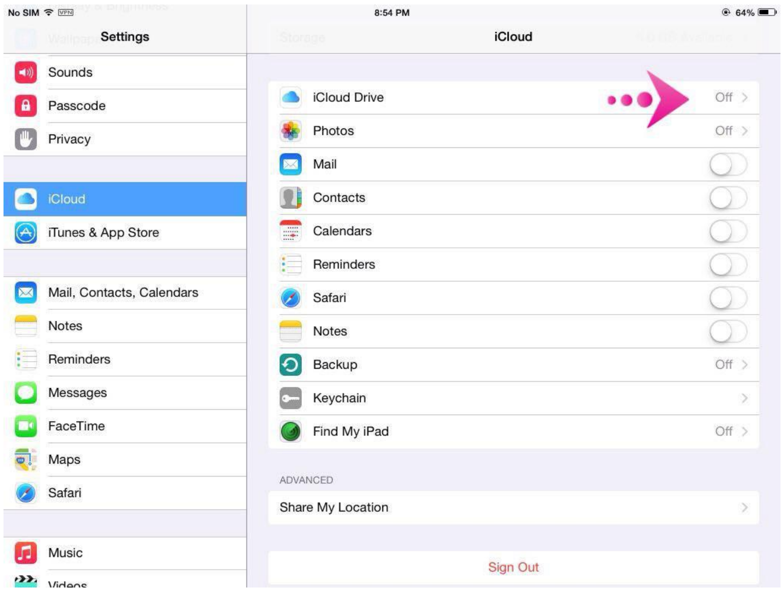


2

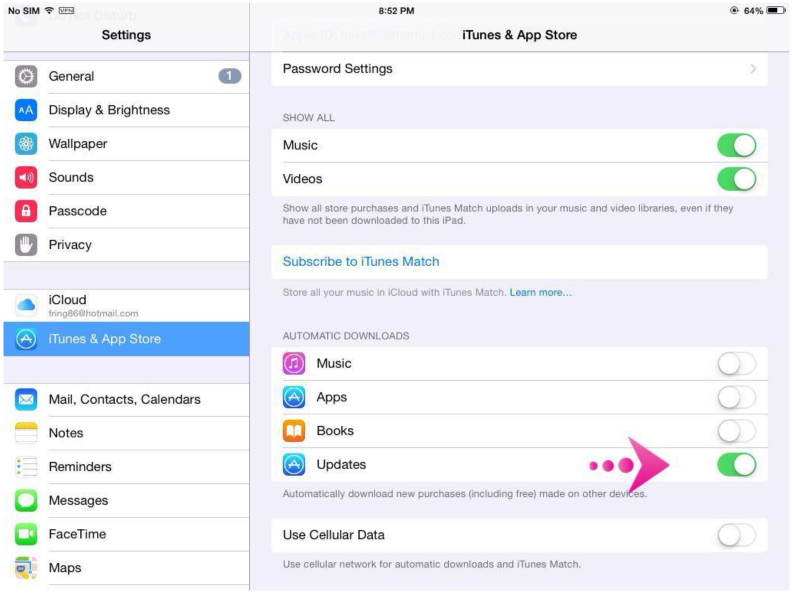


اس سے یہ ہوتا ہے کہ ایڈز یعنی اشتہارات جو اکثر لوگوں کے ڈیٹا یا لوکیشن تک رسائی حاصل کرتے ہیں،یہ ان کو محدود کرتا ہے۔

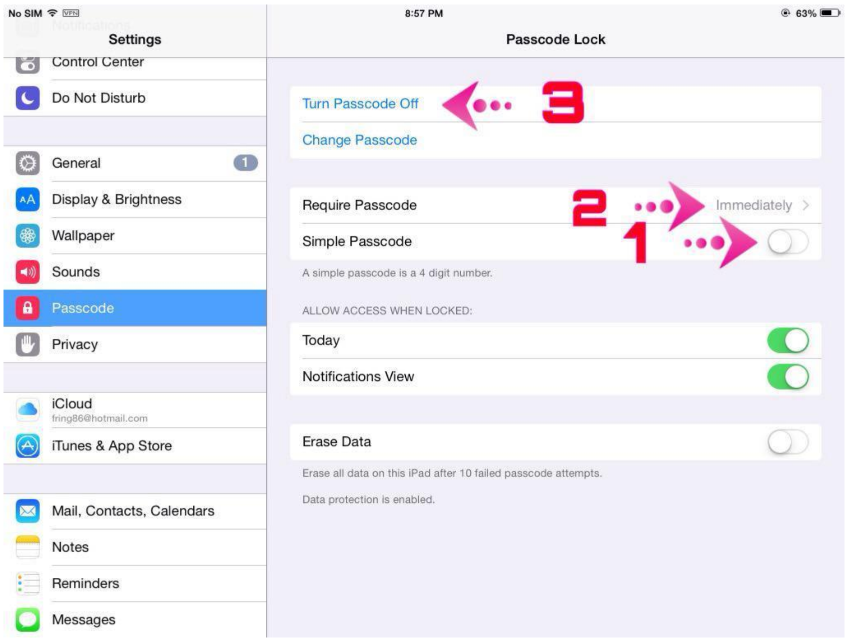
۴: iCloud کو بند کرنا: پرائویسی کے بعد اب اس کے نیچے iCloud پہ کلک کریں اور اس میں سے iCloud drive کے آپشن کو Off کریں۔آئی کلاوڈ ڈرائیو محفوظ نہیں ہے اس لئے اس کا اکاونٹ نہ بنائیں اور وہاں چیزیں بھی اپلوڈ نہ کریں۔



۵۔آٹومیٹک اپڈیٹس کو On کرنا: اپڈیٹس میں عموماً سیکیورٹی کو بہتر بنائی جاتی ہے،اس لئے موبائل کو اپڈیٹ کرتے رہیں۔اس کے لئے سیٹنگز میں iTunes & App Store پہ کلک کریں اور اپڈیٹس کو On کریں۔

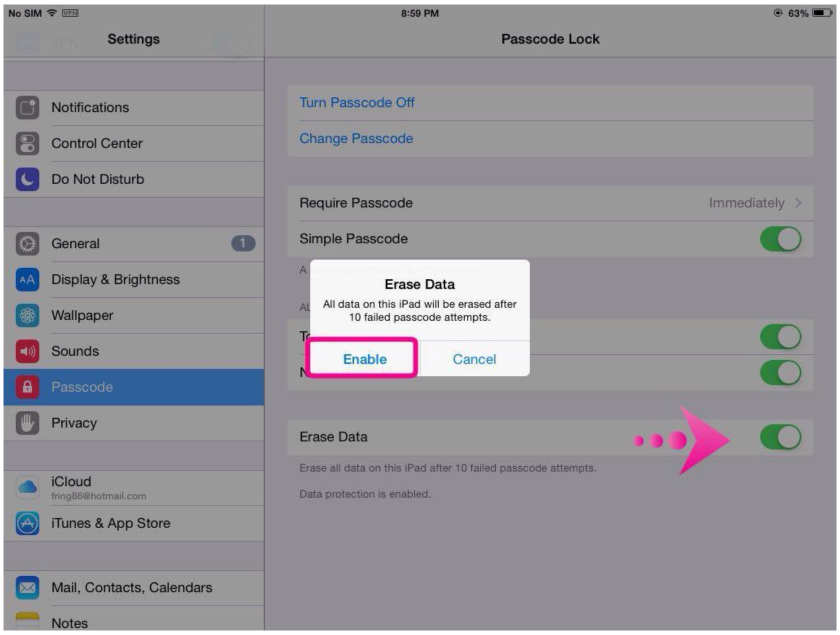


۶۔پاسورڈ سیٹ کرنا: موبائل گُم یا چوری ہونے کی صورت میں یا پولیس یا ایجنسی کے ہاتھ لگنے سے آپ کے ڈیٹا ان کو نہ مل جائیں،اس کے لئے ایک مضبوط پاسورڈ سیٹ کریں۔اس کیلئے سیٹنگز میں جائیں پھر اس میں پاس کوڈ میں جائیں،پہلے سیمپل پاسورڈ کو بند کردیں اور require password پہ کلک کرکے اس کو immediately پہ سیلیکٹ کریں،پھر اس کے اوپر Turn password on پہ کلک کریں اور ایک پاسورڈ ڈال دیں جو کم از کم 8 حروف پر مشتمل ہو اور اس میں اس طرح کے حروف بھی ڈالیں $#@@%۔



جب آپ پاسورڈ ڈال دینگے تو یہ لکھا آئے گا کہ Data protection is enabled۔

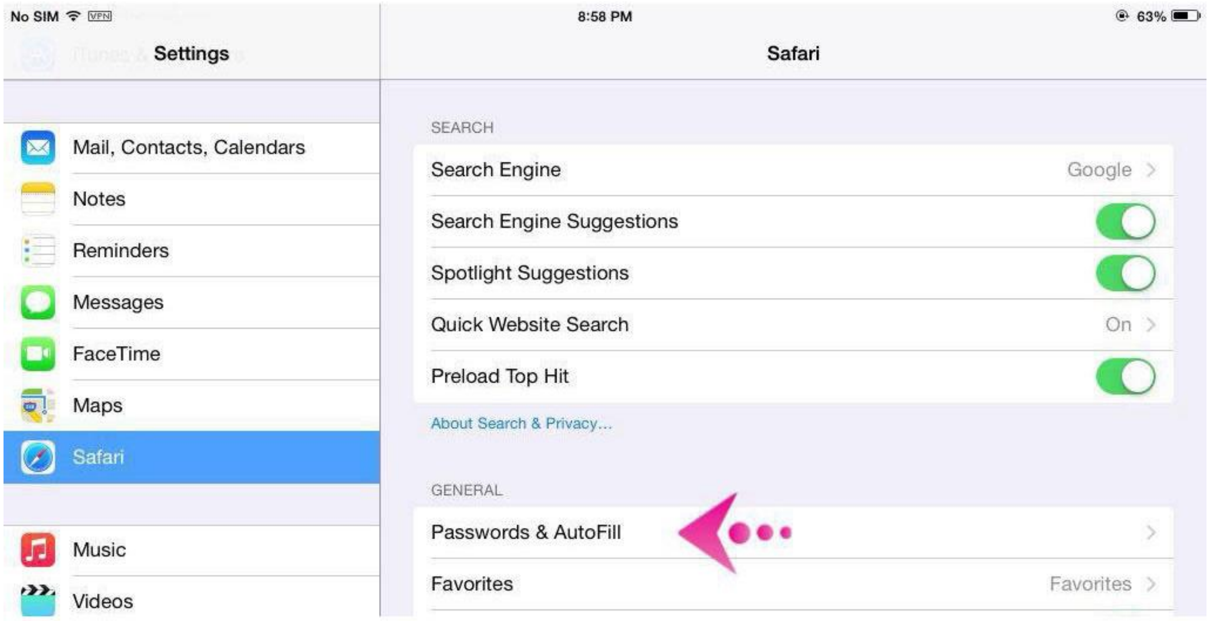
اگر آپ کا موبائل صرف آپ ہی استعمال کرتے ہیں اور وہ بچوں کی پہنچ سے دور ہے تو آپ اس میں مزید احتیاط کر سکتے ہیں Erase data کے آپشن کو استعمال کر کہ اس سے یہ ہو گا کہ اگر کوئی دس مرتبہ غلط پاسورڈ لگائے تو اس فون میں تمام ڈیٹا خود بخود ڈیلیٹ ہو جائینگے۔ اس کیلئے آپ اسی پاس کوڈ کے خانے میں Erase Data پہ کلک کریں اور enable پہ کلک کریں جیسے نیچے تصویر میں دکھایا ہے۔



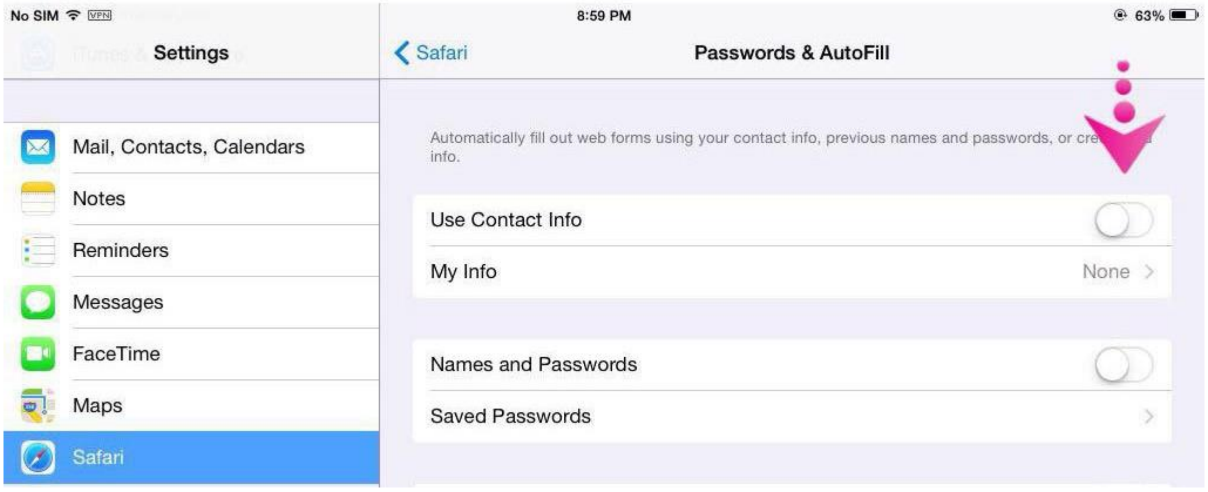
۷۔ براوزر کے سیٹنگز اور براوزر کا انتخاب: چونکہ iOS میں سفاری براوزر پہلے سے ہی انسٹال ہوا آتا ہے تو بہتر یہی ہے کہ اسی کو استعمال کیا جائے، کیونکہ یہ تھوڑا بہت سیکیور ہے، باقی بس اس کے سیٹنگز میں یہ تبدیلی کر دیں۔

سب سے پہلے آپ اپنے فون کے سیٹنگز میں جائیں، پھر اس میں سفاری/ Safari پہ کلک کریں، اس میں Passwords & Autofill پہ کلک کریں، پھر اس میں جتنے بھی آپشن ہیں سب کو Off کریں یا None پہ رکھیں، جیسا نیچے تصویر میں دکھایا ہے۔

1



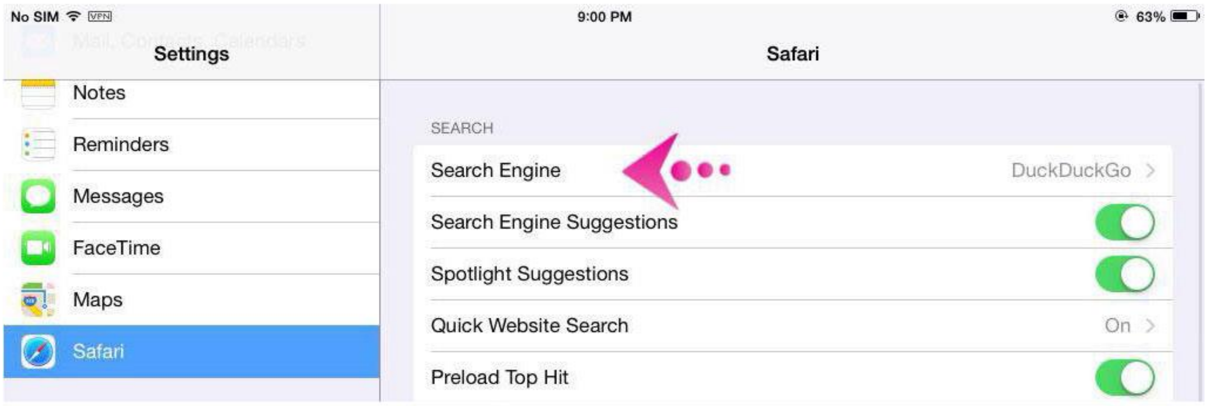
2



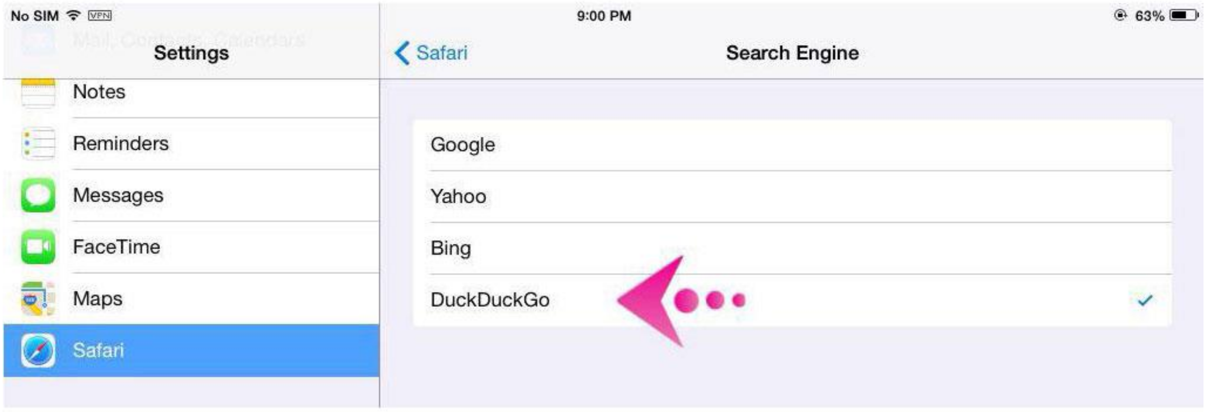
جیسا کہ پچھلے اسباق میں بتا چکا ہوں کہ کچھ کمپنیاں اپنے صارفین کی مکمل معلومات لیتے ہیں جس میں گوگل سرفہرست ہے، اور وہ دوسرے حکومتوں کو یہ معلومات فراہم بھی کر سکتے ہیں، اس لئے بہتر یہی ہوگا کہ آپ گوگل استعمال نہ کریں، یعنی انٹرنیٹ میں سرچ کرنے کیلئے گوگل کی بجائے دوسرا کوئی سرچ انجن استعمال کریں۔ سب سے محفوظ سرچ انجن "ڈک ڈک گو" ہے، اس لئے اپنے براوزر کا سرچ انجن اسی پہ رکھیں۔

اس کیلئے آپ اسی سفاری کے سیٹنگز میں search engine پہ کلک کریں، اور اس میں آپ Duck Duck Go پہ کلک کریں۔

1



2

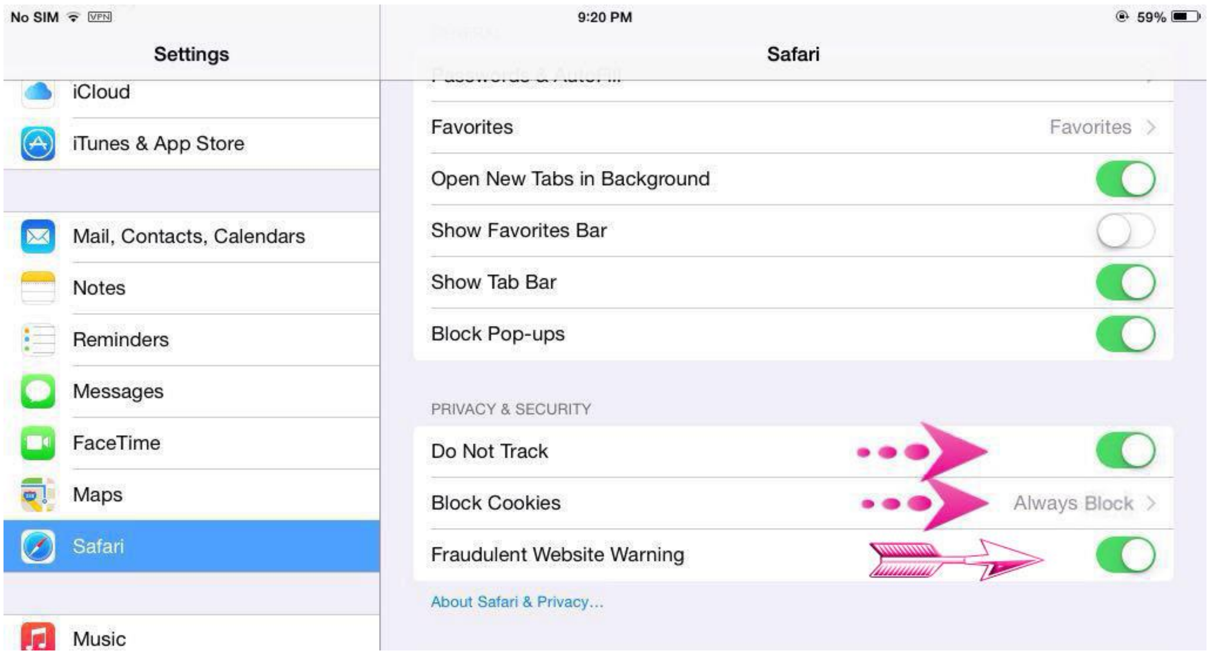


اگرچہ یہ گوگل کی طرح تیز اور چیزیں نہیں ڈھونڈ سکتا، مگر احتیاط اسی میں ہے کہ اس کا استعمال کیا جائے اگرچہ یہ اس کا اچھا متبادل نہیں۔

باقی اب براوزر کی سیٹنگز میں پرائویسی اینڈ سیکیورٹی سیٹنگز کے اندر Do not Track والے آپشن کو On کریں، اس سے ویب سائٹ آپ کی لوکیشن معلوم نہیں کر سکینگی۔

دوسرا اس میں Block cookies کو Always Block پہ رکھیں، اس سے براوزر کوکیز کو سیو/محفوظ نہیں رکھیگا جس میں یہ معلومات ہوتی ہیں کہ آپ نے کس کس ویب سائٹ کو دیکھا ہے۔

تیسرا آپ اس میں Fraudulent Website Warning والے آپشن کو On پہ رکھیں، اس سے یہ ہوگا کہ جو ویب سائٹ فراڈ ہوں اس براوزر کے مطابق اس پہ آپ کو ایک وارننگ/تنبیہ آئیگی کہ اس ویب سائٹ پہ نہ جائیں۔



اس کے علاوہ براوزر آپ سیف براوزر استعمال کر سکتے ہیں جو کسی حد تک محفوظ ہے اور اس کے علاوہ 'اوپرا منی' بھی استعمال کر سکتے ہیں۔

Safe browser کا لنک:

https://itunes.apple.com/gb/app/kaspersky-safe-browser-fast/id723879672?mt=8

Opera Mini کا لنک:

https://itunes.apple.com/gb/app/opera-mini-web-browser/id363729560?mt=8

پراکسی یعنی آئی پی ایڈریس تبدیل کرنے کیلئے سافٹوئیر کا استعمال

جیسا ہمیں معلوم ہے کہ سب سے محفوظ نیٹ ورک 'ٹور' کا ہوتا ہے مگر چونکہ آئی فون میں 'ٹور براوزر' فری میں نہیں ملتا اور اسے استعمال کرنے کیلئے فون کو جیل بریک کرنا پڑتا ہے اور جیل بریک کے بعد بھی اس کے چلانے میں مسئلہ پیش آتا ہے اس لئے ہم اس کا استعمال نہیں کرینگے۔

پراکسی سافٹوئیر iOS میں دو سافٹوئیر ایسے ہیں جو کافی حد تک محفوظ ہیں، لیکن وہ فری نہیں ہیں ان کو صرف کچھ مدت کیلئے فری میں استعمال کر سکتے ہیں مگر کچھ کوڈ ڈالنے سے ان کو زیادہ مدت تک استعمال کر سکتے ہیں۔ان میں سے پہلا سافٹوئیر یہ ہے:

الف: ایف سیکیور فریڈوم: اس کو یہاں سے ڈاونلوڈ کریں

https://itunes.apple.com/gb/app/f-secure-freedome-vpn/id771791010?mt=8

ڈاونلوڈ کرنے کے بعد اسے کھولیں، ایک اسکرین آئیگی ٹورئیل کیلئے اسے اسکپ کر دیں۔
پھر اس کے کھلنے کے بعد اب کوڈ ڈالنے کیلئے اس میں ڈراپ مینیو یعنی تین لکیروں والے آپشن کو کلک کریں جیسا نیچے تصویر نمبر ۲ میں دکھایا ہے۔
پھر اس میں سبسکرپشن پہ کلک کریں۔

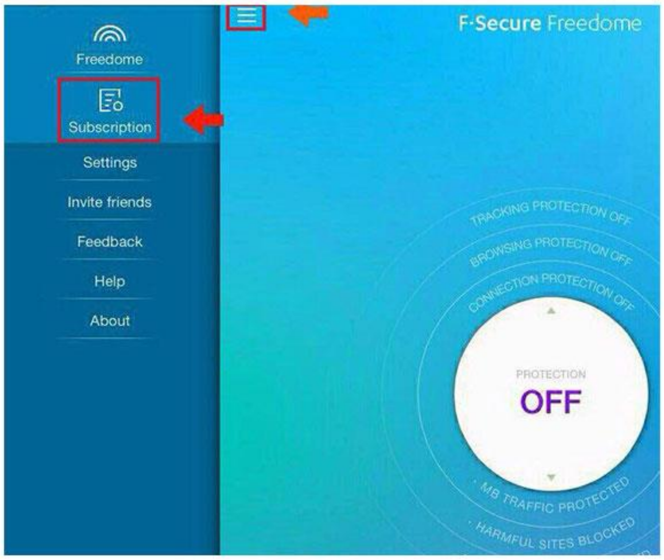
پھر ہیوا ے کوڈ/ have a code پہ کلک کریں۔

پھر ایک کوڈ لکھنے کی جگہ آئیگی اس میں یہ کوڈ ڈالیں۔

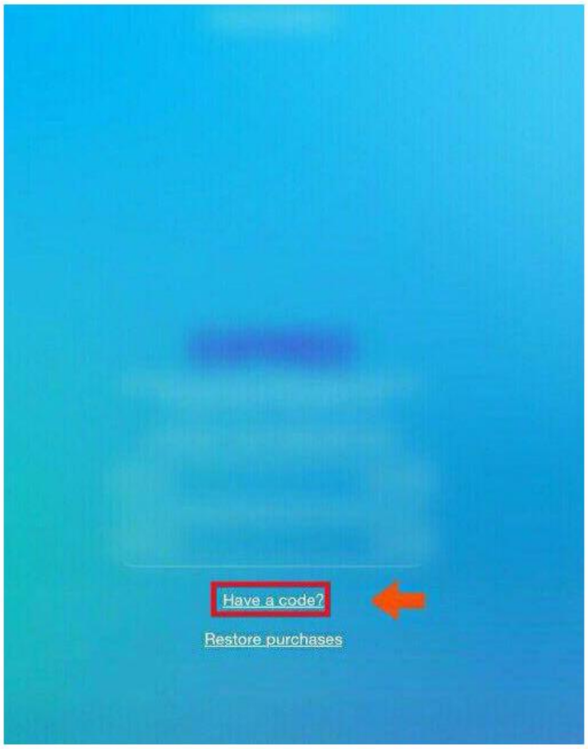
w9f4ct

1

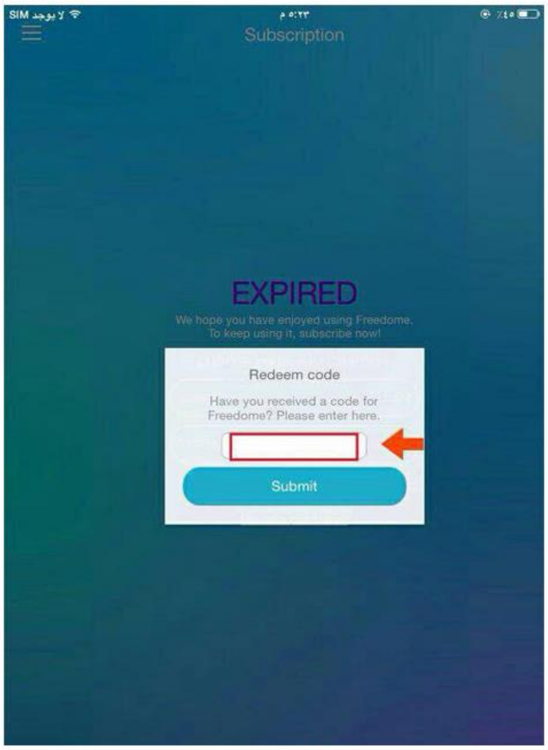
2



3



4



اب آپ اس کو تین مہینے تک استعمال کر سکینگے۔
اس کو چلانے کیلئے Off پہ کلک کریں On لکھا نظر آئیگا یعنی اب چل رہا ہے، اور نیچے لوکیشن پہ کوئی سا بھی لوکیشن سیلکٹ کریں۔

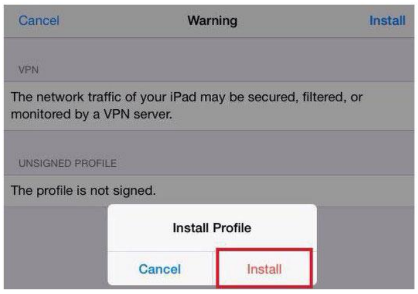
ب: آواسٹ سیکیورلائن: یہ بھی آئی پی ایڈریس تبدیل کرنے کی ایک ایپ ہے جو کہ آواسٹ کمپنی کی ہے۔ اس کو یہاں سے ڈاونلوڈ کریں

https://itunes.apple.com/gb/app/secureline-vpn-wifi-security/id793096595?mt=8

انسٹال کرنے کے بعد اسے کھولیں، جب آپ اسے کھولینگے تو ایک اسکرین نظر آئیگی جس میں لکھا ہوگا کہ اس وی پی این کو چلانے کیلئے آپ کو پروفائل انسٹال کرنا ہوگا، تو آپ اس میں Install profile پہ کلک کریں، اس کے بعد پھر ایک اسکرین آئیگی اس میں install پہ کلک کریں، اس طرح دو اور اسکرین آئینگی دونوں میں آپ نے install پہ کلک کرنا ہوگا، پھر وہ پروفائل انسٹال ہوگا۔

1

2



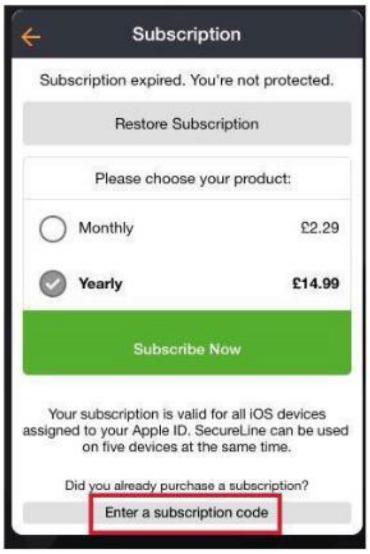
3

اس سافٹوئیر کو بھی چونکہ ایک ہفتے کیلئے فری استعمال کر سکتے ہیں اس لئے ہم اس میں بھی ایک کوڈ کا استعمال کرینگے جس سے ہم اس کو مزید تین، چار سال تک استعمال کر سکینگے۔
اس کیلئے آپ نیچے دیے گئے تصویر کو ملاحظہ فرمائیں۔

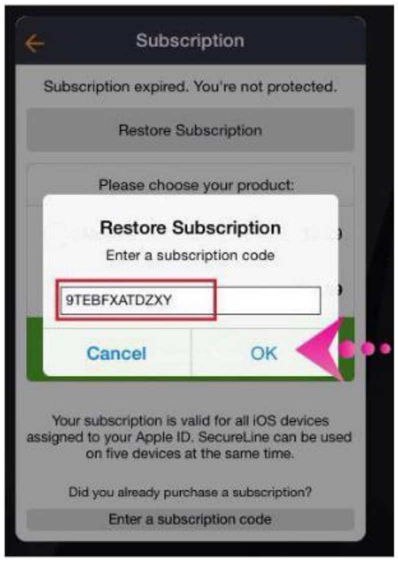
1

2

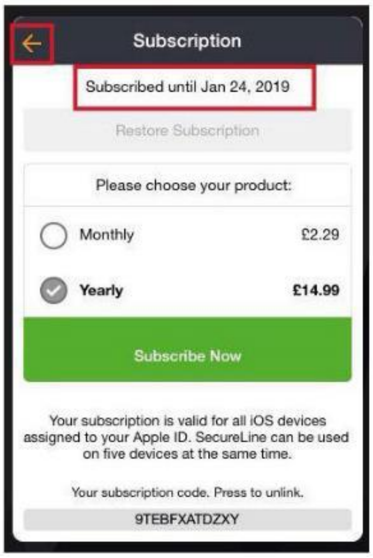
3



4



5



6

یعنی پہلے سیٹنگز میں جائیں، پھر سبسکرپشن پہ کلک کریں، پھراس میں اِنٹراے سبسکرپشن کوڈ پہ کلک کریں، پھر یہ کوڈ ڈالیں

9TEBFXATDZXY

اب آپ اس کو کئی سالوں تک مفت استعمال کر سکتے ہیں، اب اس کو چلانے یا کنیکٹ کرنے کیلیئے یہاں سے پیچھے جائیں اور مین اسکرین پہ کنیکٹ پہ کلک کریں، جب صحیح کا نشان آیئگا تو سمجھ لیں کہ چل رہاہے۔

نوٹ: جب ان دونوں سافٹوئیر کو چلاوگے تو یہ چیک کرنے کیلیئے کہ واقعی یہ آئی پی ایڈریس تبدیل کر رہے ہیں یا نہیں، اس کیلیئے اس لنک پہ جائیں دیکھیں کہ کونسا آئی پی دکھا رہا ہے اور لوکیشن کیا بتا رہاہے۔

http://www.whatismyipaddress.com

یہاں تک آئی فون اور آئی پیڈ کی سیکیورٹی کا اختتام کرتے ہیں، باقی آپ اینڈرائیڈ سیکشن میں دیکھ سکتے ہیں کہ مزید کیا کیا کرنا ہے، مثلاً بی بی ایم کا استعمال اور ٹیلیگرام کا استعمال وغیرہ۔

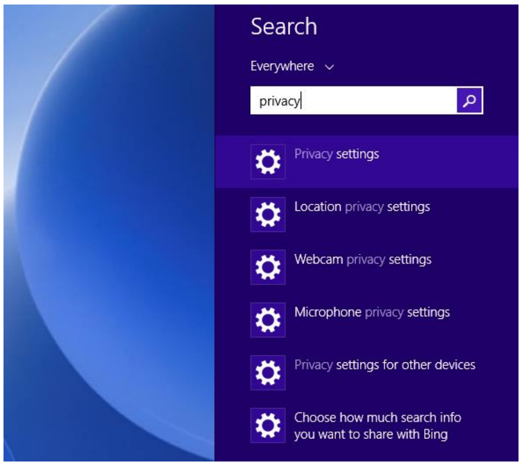
سیکشن دوم۔۔۔۔۔۔۔۔۔۔

کمپیوٹر سیکیورٹی

ونڈوز کی سیکیورٹی:

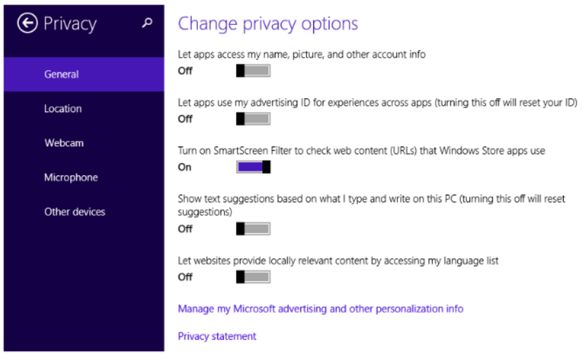
کمپیوٹر میں جتنا نیا یا اپڈیٹڈ آپریٹنگ سیسٹم مثلاً ونڈوز، لینکس وغیرہ استعمال کریں اتنا ہی بہتر ہے۔ویسے تو لینکس کی سیکیورٹی ونڈوز سے کافی بہتر ہے مگر چونکہ اکثریت ونڈوز ہی استعمال کرتی ہے، اس لئے اس سیکشن میں ہم کمپیوٹر میں صرف ونڈوز سے متعلق بات کرینگے۔ چونکہ لینکس کا استعمال کرنے والے کمپیوٹر میں پہلے سے مہارت رکھتے ہیں ان کو ان باتوں کی ضرورت بھی نہیں ہوگی، رہی بات میک / Mac استعمال کرنے والوں کی وہ اس سے اندازہ لگا کر بھی اپنے سیکیورٹی سخت کر سکتے ہیں۔

۱۔ **Windows 8 یا اس سے اوپر والوں میں لوکیشن وغیرہ کو بند کرنا:** سب سے پہلے search میں جائیں اور وہاں لکھیں Privacy settings پھر اس پہ کلک کریں جیسا تصویر میں دکھایا ہے۔

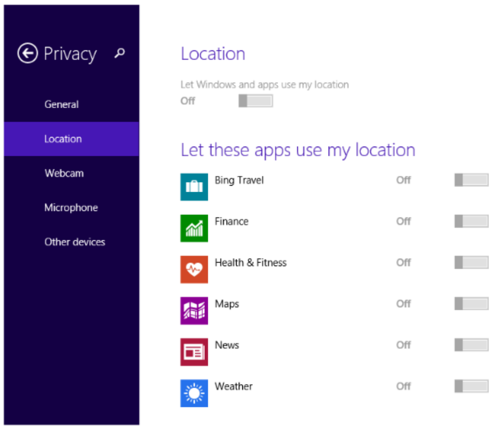


پھر اس میں سیٹنگز کو ایسا کریں جیسے نیچے تصویر میں دکھایا ہے۔یعنی General میں سب کو Off کریں سوائے Smart Screen Filter کو۔

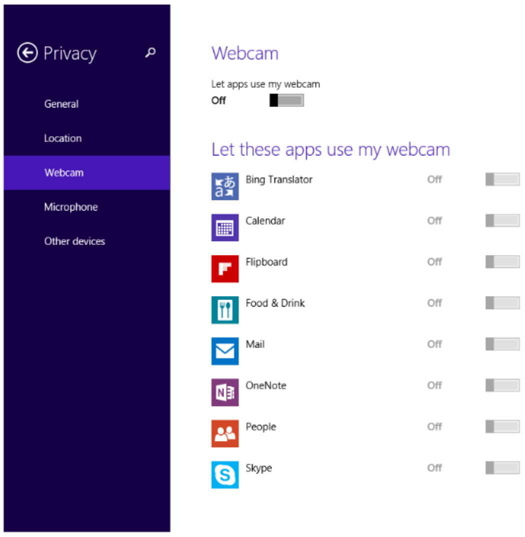
1



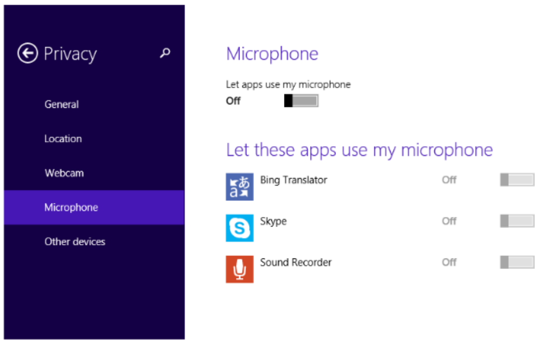
2



3



4



Location پہ کلک کریں اور اس کو Off کریں۔

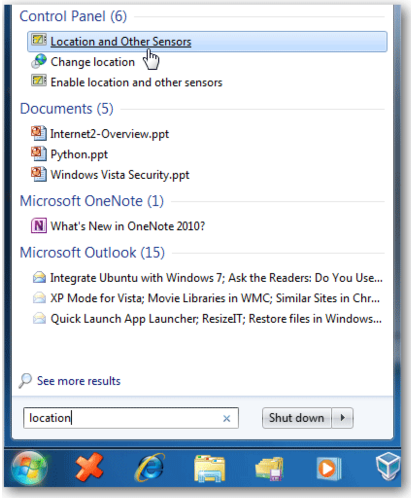
پھر webcam پہ کلک کریں اور اسے بھی Off کریں۔ اگر آپ Skype وغیرہ استعمال کرتے ہوں تو صرف استعمال کرتے وقت ان کو On کریں۔۔

پھر Microphone پہ کلک کریں اور Off کریں۔

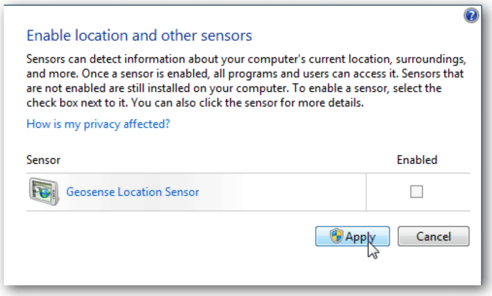
نوٹ: جو لوگ مجاہدین سے رابطے میں ہیں اور ان سے مدد وغیرہ بھی کرتے ہیں، یعنی میڈیم اور ہائی پروفائل کے لوگ صرف ان سیٹنگز پہ اکتفاء نہ کریں بلکہ اپنے لیپ ٹاپ کے ویب کیم پہ ٹیپ لگائیں۔ اور اسپیکر کے خانے میں ایئر فون ڈالیں اور آپشن میں مائک سیلکٹ کریں، تاکہ بالفرض کل کو آپ کی جاسوسی ہوتی ہے ہیکنگ کے ذریعے تو کم از کم کیمرہ اور مائک تو کام نہ کریں۔

Windows 7 میں ان سیٹنگز کا طریقہ: ونڈوز 7 میں یہ سیٹنگز تو موجود نہیں البتہ کسی کسی میں لوکیشن کی سیٹنگز ہیں۔
اس کے لئے آپ پہلے Start پہ کلک کریں Search خانے میں لکھیں Location، پھر Location and Other Sensors پہ کلک کریں

1



2



اگر Geosense Location Sensor پہ Enabled پہ صحیح کا نشان نہیں لگا تو رہنے دیں اگر لگا ہے تو اسے ختم کر دیں اور پھر Apply پہ کلک کریں۔

ضروری نہیں کہ یہ آپشن ونڈوز 7 کے سب ورژن میں ہو، یہ کسی کسی ورژن میں ہوتا ہے۔

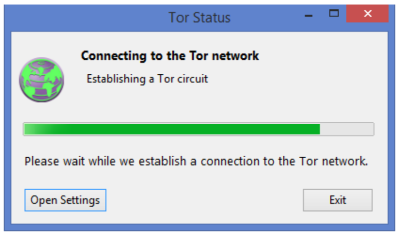
براوزر کے سیٹنگز اور براوزر کا انتخاب

TOR کا استعمال: یہ سب سے زیادہ محفوظ براوزر و محفوظ پراکسی (آئی پی ایڈریس تبدیل کرنے کا) سافٹویر ہے۔اس کو یہاں سے ڈاونلوڈ کریں:

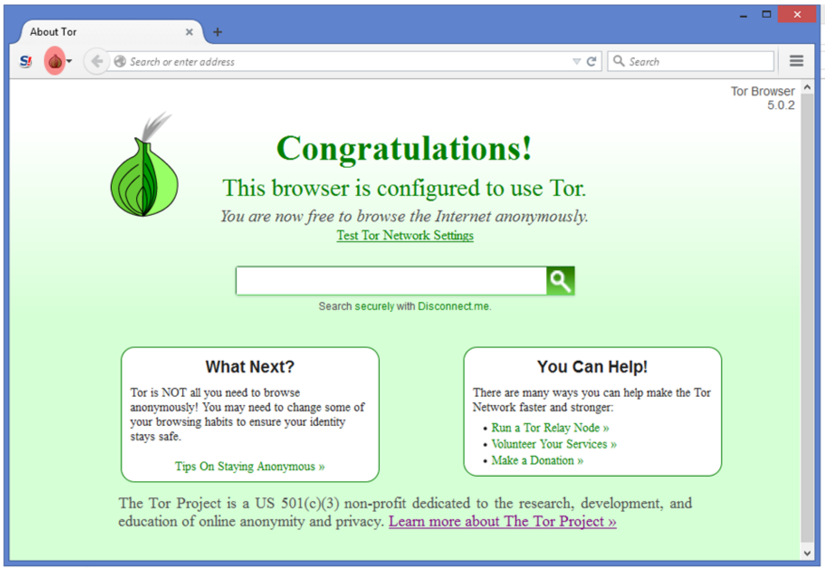
https://www.torproject.org/download/download-easy.html.en

ڈاونلوڈ کرکہ انسٹال کریں،اوراس کو چلائیں۔یہ اسکرین آئیگا۔

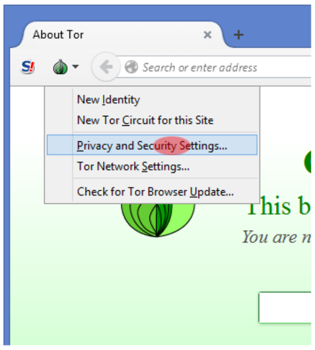
1



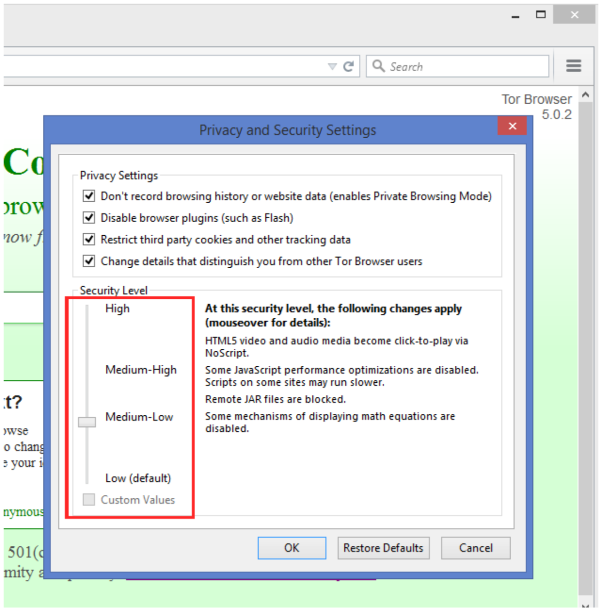
2



3



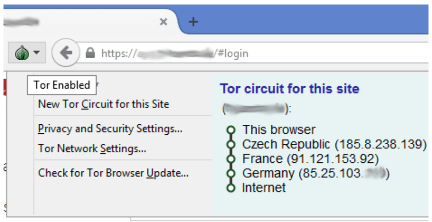
4



جیسا تصویر ا میں دکھایا ہے شروع میں یہ اسکرین آئیگا یعنی Tor کنیکٹ ہورہا ہے،پہلی مرتبہ تھوڑا دیر کریگا،بعد میں پھر جلدی کھلیگا،پھر جب کنیکٹ ہوجائیگا تو تصویر ۲ جیسا اسکرین آئیگا یعنی اب یہ براوزر Tor پہ چل رہاہے اب اس کا استعمال کر سکتے ہیں۔

اس میں سیکیورٹی کو مزید سخت کرنے کیلئے پیاز والے نشان پہ کلک کریں جیسا تصویر ۲ میں دکھایا ہے۔ پھر Privacy and Security Settings پہ کلک کریں۔
پھر سیکیورٹی لیول کو دیکھیں جس قدر آپ سیکیورٹی دینا چاہتے ہیں دے دیں، جتنا بڑھائینگے ویب سائٹ اتنا سستی سے کھلینگے اور بعض ویب سائٹ صحیح نہیں کھلینگے تو عام تور پر Medium Low پہ رکھیں۔

نوٹ: ویسے عام طور پر Low پہ ہوتی ہے اور اگر اس کے اس سیٹنگز کو تبدیل نہ بھی کریں تب بھی صحیح ہے۔ Low پر بھی ہو تو تب بھی سیکیورٹی سخت ہی ہوتی ہے کیونکہ ٹور ایک برج سے دوسرے اور دوسرے سے تیسرے پہ اور پھر انٹرنیٹ کا استعمال کرتی ہے جیسا اس تصویر میں دکھایا ہے



اور براوزر کو بھی اپنے سیکیور ترین سیٹنگز پہ رکھتی ہے، یہ مزید سیکیورٹی ان کی لئے ہے جو بڑے ہیکرز سے بچنا چاہتے ہیں، اور ایسے ہیکر پاکستان میں تو مشکل ہے ایسے ہوں۔ اس لئے Medium Low پہ رکھیں زیادہ مناسب ہے اور اگر Medium Low پہ بھی کوئی ویب سائٹ صحیح نہیں کھل رہا اور آپ کو وہ چلانا ہو تو آپ Low پہ ہی رکھیں کوئی مسئلہ نہیں۔
ٹور کی سیکیورٹی باقی عام پراکسی سافٹوئیر سے ۱۰ گنا بہتر ہے۔

Tor سے محفوظ طریقے سے فیسبوک استعمال کرنے کے لئے یہ لنک استعمال کریں: https://www.facebookcorewwwi.onion

اس لنک کا فائدہ یہ ہے کہ اس سے آپ کی کوئی بھی آئی پی ایڈریس فیسبوک والوں کے پاس نہیں جا گی، نہ اصلی اور نہ پراکسی والی۔ یہ ٹور ہی کے سرور کے ذریعے فیسبوک استعمال کرتی ہے۔ اگر آپ اس کا کنیکٹ ہونے کا ڈاگرام دیکھیں تو اس طرح نظر آئیگا کہ ایک برج سے دوسرے برج، دوسرے سے تیسرے پھر ریلے کا استعمال ہوگا جن میں ایک ریلے سے دوسرے، دوسرے سے تیسرے اور پھر فیسبوک۔ ریلے کے ذریعے فیسبوک کے پاس آئی پی ایڈریس نہیں جا گی۔
اس کا فائدہ یہ ہے کہ عام طور پر جب آپ مختلف ممالک کے آئی پی ایڈریس استعمال کرتے ہیں تو فیسبوک آپ کو بلاک کرتی ہے اور کچھ سیکیورٹی سوال کرتی ہے اور بعض اوقات بغیر سوال کہ صرف آئی ڈی کارڈ اپلوڈ کا کہتی ہے جس سے یقینی طور پر فیسبوک کا بلاک کرنا ہی مراد ہے۔ تو اس لنک کے ذریعے سے استعمال کرنے میں آپ کو کوئی مسئلہ پیش نہیں آئیگا اگر فیسبوک آگے کوئی اقدام نہ کرے تو۔

عام براوزر میں آپ اس لنک میں نہیں جا سکتے۔

ہمیشہ Tor کا اپڈیٹڈ ورژن استعمال کریں، اور اپڈیٹ کرتے رہیں۔

ایک شبہ اور اس کا جواب: یہاں یہ سوال پیدا ہو سکتا ہے کہ TOR یہ سب کچھ مفت میں کیوں دے رہی ہے حالانکہ دوسرے پراکسی سافٹوئیر تو پیسے لے کر بھی کم سیکیورٹی دیتے ہیں، اور ٹور کس طرح کمائی کرتی ہے؟
تو اس کا جواب یہ ہے کہ ٹور کو ایک امریکی ادارے نے بنایا تھا اور وہی اس کو فنڈنگ کرتے تھے اور یہ لوگوں کے ڈونیشن یعنی چندے بھی لیتی ہے، بڑے بڑے ادارے بھی ان کو بہت زیادہ ڈونیشن دیتے ہیں اس سروس فراہم کرنے کے بدلے۔ ان سب کا مقصد بھی یہی ہے کہ لوگوں کی پرائویسی/رازداری محفوظ رکھنے کیلئے ان کو یہ سروس مفت میں ملے۔ اور ٹور کو ان ڈونیشن/چندے سے اتنے پیسے ملتے ہیں شاید دوسرے پراکسی سافٹوئیر والوں کو پیسے پہ بیچنے پر بھی نہیں ملتے۔ البتہ ایک شبہ یہ ہو سکتا ہے کہ اس کو سب سے زیادہ فنڈنگ امریکی ایک سیکیورٹی ادارہ کر رہا ہے تو کیا یہ ان کیلئے جاسوسی نہیں کر سکتی؟ تو اس میں یہ بتاتا چلوں کہ جتنے بھی ہیکرز ہیں ان میں سے اکثریت ٹور پر بھروسہ کرتے ہیں اور یہ

بھروسہ اس کو آزمانے کے بعد ہی کرتے ہیں، چونکہ بلیک ہیٹ ہیکرز بھی اپنے اپنے ممالک کے سیکیورٹی اداروں سے یا سی آئی اے سے چھپے ہوتے ہیں، ان کا بھی جرم بہت بڑا ہوتا ہے اور وہ ٹور ہی استعمال کرتے ہیں۔ تو ہم ان کے تجربے پر تھوڑا بہت بھروسہ کر سکتے ہیں۔ البتہ مکمل بھروسہ اس پہ بھی نہیں ہو سکتا۔

نوٹ: بعض حضرات zenmate کا استعمال کرتے ہیں اور دوسروں کو مشورہ بھی دیتے ہیں، تو اس کے متعلق بتاتا چلوں چونکہ وہ بھی مفت سروس فراہم کر رہا ہے مگر اس کا مقصد آپ کی لاگ کو امریکہ کی ایجنسی کو بیچنا ہی ہے، اس پر بقاعدہ تحقیق ہوئی ہے۔ لہذا اس کو استعمال نہ کریں۔ اور دوسرے اس طرح کے مفت سروس دینے والوں کو بھی استعمال نہ کریں جب تک تحقیق نہ کریں۔

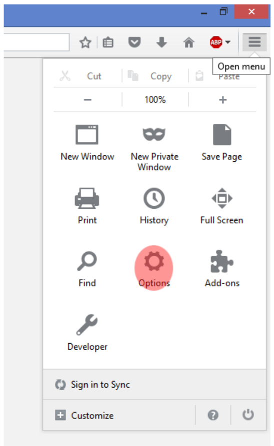
اور ایک بات کہ جو سافٹوئیر کریک ہوئے ہوں وہ دراصل مفت نہیں ہیں، بلکہ ان کو ہیک کر کہ مفت بنایا جاتا ہے، اس لئے ان کو مفت نہ سمجھیں۔

دیگر براوزرز کا انتخاب اور ان کے سیٹنگز

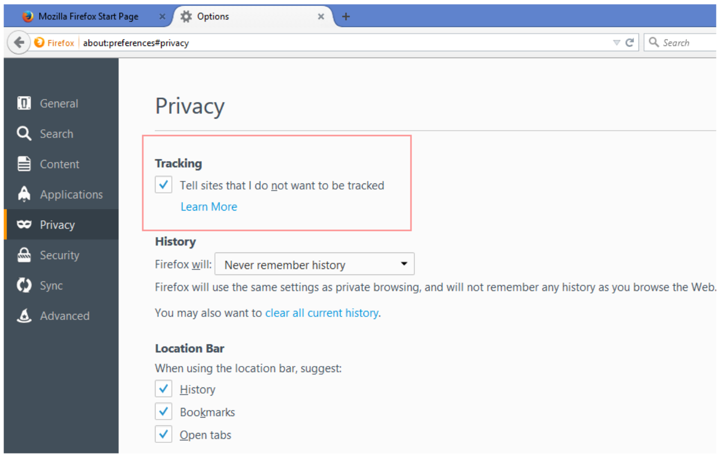
اگر آپ کے نیٹ کا سپیڈ سست ہے اور TOR چلانے میں مشکل ہو رہی ہو تو آپ F Secure Freedome انسٹال کر کہ (انسٹال کرنے کا طریقہ آگے بتائینگے) اس کے ساتھ فائرفوکس یا کُروم یا اوپرا کا استعمال کریں، تینوں کی اپنی اپنی خوبیاں اور خامیاں ہیں البتہ Firefox بہتر ہے۔

ا۔ فائرفوکس/ Firefox: سب سے پہلے لوکیشن ٹریس ہونے والے آپشن کو ختم کریں، اس کیلئے یہ تصویر دیکھیں۔

1



2



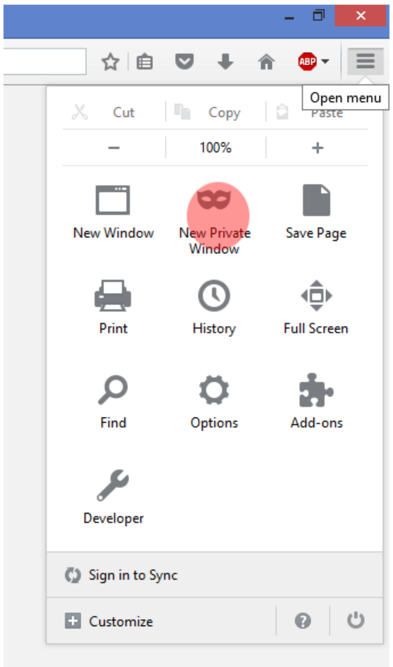
یعنی پہلے براوزر کے مینیو میں جائیں پھر اس میں Options کو کلک کریں، پھر اس میں سے Privacy کو کلک کریں پھر Tracking والے آپشن میں دیکھیں اس آپشن کو صحیح کا نشان لگائیں جیسا تصویر ۲ میں دکھایا ہے۔

اگر آپ مزید احتیاط کرنا چاہتے ہیں تو اسی سیٹنگز میں History کو Never remember history پہ سیلکٹ کریں ویسے اس سے بہتر طریقہ یہ ہے کہ آپ Private window کھولیں۔

اس کا طریقہ یہ ہے آپ براوزر کے مینیو میں جائیں، پھر اس میں New Private window پہ کلک کریں۔

اس میں یہ ہوتا ہے کہ اس سے آپ کا براوزر اس کی ہسٹری، پاسورڈ، کوکیز، ٹیمپیرری فائلز وغیرہ کچھ بھی محفوظ نہیں کرتی۔

اس سے آپ کسی حد تک محفوظ رہتے ہیں۔ مگر اس سے ویب سائٹ تھوڑا سستی سے کھلینگے کیونکہ دوسرے طریقے سے جب آپ ایک ویب سائٹ کو دوسری مرتبہ کھولتے ہیں تو وہ ٹیمپیرری فائلز کو لوڈ کرتا ہے جو پہلے محفوظ ہو چکے ہیں اور اس طرح ویب سائٹ جلد کھل جاتا ہے، مگر اس طریقے سے ہر بار اس کو اس ویب سائٹ کے تمام فائل لوڈ کرنے پڑتے ہیں۔

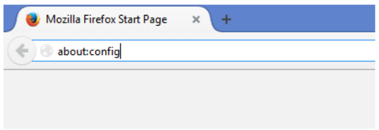


ایک براوزر پر کئی فیسبوک اکاونٹ کھولنے کیلئے بھی یہ طریقہ مفید ہے،یعنی ایک اکاونٹ کھولا اور پھر لاگ آوٹ ہوئے پھر اسی براوزر پر دوسرا اکاونٹ کھولا،اس کیلئے یہ طریقہ استعمال کریں کیونکہ دوسرے طریقے سے پھر فیسبوک آپ کو سیکیورٹی سوال کر سکتا ہے کیونکہ اس سے آپ مشکوک ہوتے ہیں کہ ایک ہی براوزر سے کئی اکاونٹ۔اور فیسبوک ڈاریکٹ کوکیز تک رسائی حاصل کرتی ہے اگر پہلے موجود ہوں۔اس طرح آپ نے اگر ایک فیک اکاونٹ بنایا ہے اور ایک اصل اکاونٹ ہے تو فیس بک کو پتا چل جاتا ہے کہ یہ ایک ہی کمپیوٹر سے استعمال ہوے ہے اور ایک ہیکر آسانی سے معلوم کر سکتا ہے۔اس لئے بہتر یہ ہے کہ فیس بک کیلئے Private window کا انتخاب کریں اگر Tor استعمال نہیں کرتے۔

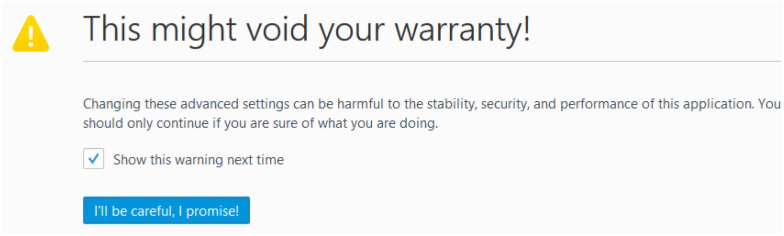
اور براوزر پہ کبھی بھی پاسورڈ محفوظ ہونے والے آپشن کو کلک مت کریں۔

WebRTC: فائر فوکس سے ویب آر ٹی سی یعنی پراکسی لگانے کے بعد اپنا اصلی آئی پی ایڈریس ظاہر ہونے والے خلاء کو بند کرنے کا طریقہ یہ ہے کہ آپ فائر فوکس کو کھولیں اور ویب سائٹ کے کانے میں یہ لکھیں

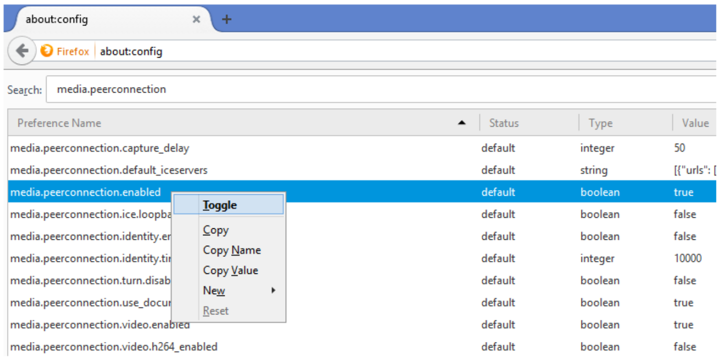
1



2



3



About:config اورانٹر کریں،پھر ایک اسکرین آئیگا جیسا تصویر ۲ میں دکھایا ہے،اس میں I'll be carefull والے آپشن کو کلک کریں پھر ایک اسکرین آئیگی اس میں سرچ کی جگہ یہ لکھیں media.peerconnection.enabled پھر اس میں دیکھیں اس نام والے خانے میں اگر value میں true لکھا ہوگا پھر اس کو رائٹ کلک کر کہ Toggle پہ کلک کریں اب اس میں False لکھا آئیگا۔اب اس کو بند کر کہ دوبارہ اسٹارٹ کریں۔اور یہ چیک کرنے کیلئے کہ واقعی بند ہوگیا ہے آپ اس لنک پہ جائیں۔

/https://diafygi.github.io/webrtc-ips

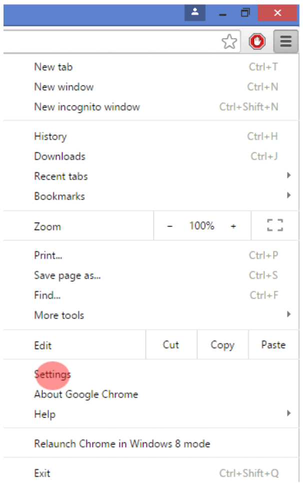
اگر اس طرح کا اسکرین آئے یعنی Ip addresses پہ خالی ہو تو Webrtc بند ہو چکا ہے۔اگر آئی پی ظاہر ہو تو بند نہیں ہوا ہے دوبارہ سے سیٹنگز دیکھ لیں اور اسے بند کر دیں۔

Adblock: اپنے براوزر میں ایڈ بلاک پلگ اِن ضرور ڈالیں،یہ Ads کو بلاک کرتی ہے اور اکثر ایڈز میں ایسے اسکرپٹ ہوتے ہیں جو لوکیشن معلوم کرتے ہیں۔اور اس سے آپ کافی حد تک جاسوسی سافٹویئر کے خودکار انسٹال ہونے سے بھی بچ سکتے ہیں۔اس لنک پہ جائیں:-https://addons.mozilla.org/en-US/firefox/addon/adblock-plus

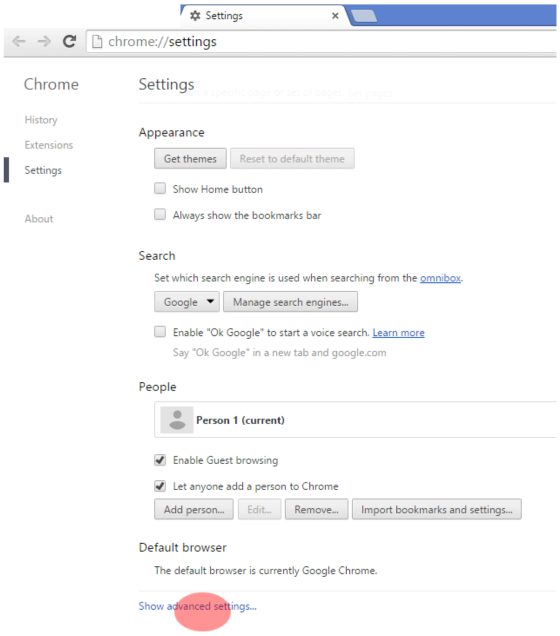
اس پہ جاکہ دیکھیں Add to firefox لکھا آئیگا،اس پہ کلک کریں،یہ اس میں انسٹال ہو جائیگا۔

۲۔Google Chrome:اس میں بھی پہلے لوکیشن ٹریس والے آپشن کو ختم کریں۔اس کیلئے آپ براوزر کھولیں، مینیو میں جائیں پھر اس میں سیٹنگز میں جائیں

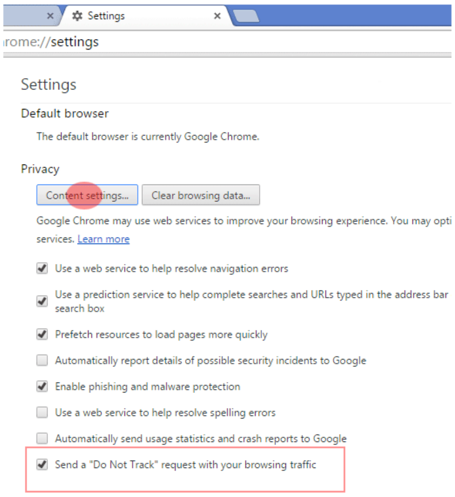
1



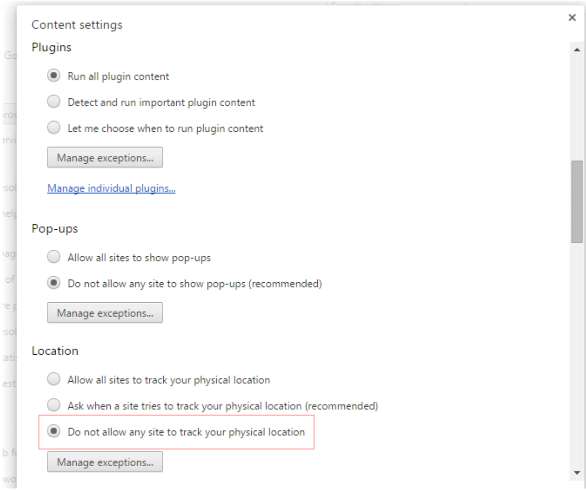
2



3



4



پھر نیچے جائیں اور Show advanced settings پہ کلک کریں، پھر اس میں نیچے دیکھیں Send a Do not track والے آپشن کو صحیح کا نشان لگائیں جیسا تصویر ۳ میں دکھایا ہے

پھر Privacy کے نیچے Content Settings پہ کلک کریں اس میں نیچے جائیں لوکیشن والے خانے میں دیکھیں Do not allow any site والے آپشن کو سیلیکٹ کریں۔

گوگل کُروم میں Private window کا نام incognito ہے،اور اس کیلئے مینیو میں جائیں جیسا تصویر 1 میں دکھایا ہے اس میں New Incognito window پہ کلک کریں۔اور پرائیویٹ وینڈو کی تفصیل فائر فاکس کے ذیل کر چکا ہوں۔اسے ضرور پڑھیں۔

WebRTC: گوگل کُروم میں webrtc کو مکمل ختم نہیں کر سکتے مگر کسی حد تک بند ہو جاتی ہے اس پلگ اِن سے،اس لنک پہ جائیں اور پلگ اِن ڈاونلود کر کہ کُروم میں ڈال دیں۔

https://chrome.google.com/webstore/detail/webrtc-leak-prevent/eiadekoaikejlgdbkbdfeijglgfdalml?hl=en

اور چیک کرنے کیلئے اُسی لنک پہ جائیں:https://diafygi.github.io/webrtc-ips/

Adblock: اس لنک پہ جاکہ Add to chrome پہ کلک کریں:

https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdccddilifddb

۳۔Opera

اوپرا میں لوکیشن ٹریس والے آپشن کو ختم کرنے کیلئے اس کو کھولیں پھر اس میں اوپر کونے میں opera لکھا ہوگا اس کو کلک کریں

پھر Settings پہ کلک کریں

پھر اس میں Privacy & Security پہ کلک کریں۔

پھر اس میں Send a Don't track والے آپشن کو صحیح کا نشان لگائیں۔

Private window کیلئے opera والے آپشن کو کلک کریں اور new private window پہ کلک کریں۔

WebRTC: اوپرا میں بھی webrtc کو مکمل بند نہیں کر سکتے بس Noscript lite پلگ ان ڈال کر کسی حد تک روک سکتے ہیں۔اس پلگ اِن کا لنک:

https://addons.opera.com/en/extensions/details/noscript-lite/?display=en

Adblock: اس لنک پہ جاکہ Add to opera پہ کلک کریں:

https://addons.opera.com/en/extensions/details/opera-adblock/?display=de

پراکسی(آئی پی ایڈریس تبدیل کرنے)کیلئے F Secure Freedome کا استعمال

اگر Tor سست ہو اور اسے استعمال کرنے میں دشواری ہو رہی ہو تو خصوصی رابطے کیلئے پھر بھی وہی استعمال کریں اور عام براوزنگ پھر ایف سیکیور فریڈوم سے کریں۔ایف سیکیور فریڈوم باقی پراکسی سافٹویر سے کافی بہتر ہے۔

ایف سیکیور فروڈوم ویسے 14 دن ٹرائل ورشن کے ساتھ آتا ہے تو ہم اُس میں کوڈ ڈالینگے جس کے ذریعے سے 30 سے 100 دن بڑھ سکتے ہیں،کوڈ اور طریقہ آگے بتائینگے۔

فریڈوم کا ڈاونلوڈ لنک:

https://download.sp.f-secure.com/freedome/installer/Freedome.exe

ڈاونلوڈ کرنے کے بعد کھولیں اور سبسکرپشن پہ کلک کر کہ ان میں سے کسی کوڈ کو ڈالیں

کوڈ کی لسٹ:

QSF257

W977SC

W9F4CT

W2PECJX

WVGXGJ

VBJCG5C

R55GVGX

R7NGWK3

AJ8R678

2BJ2U2N

9YS7Y9Y

8NNC9YT

اس سے ۳۰ سے ۶۰ دن اضافی مل سکتے ہیں، چونکہ یہ کوڈ پرانے ہیں ممکن ہے کسی بھی وقت کمپنی ان کو ختم کر لے اس لئے احتیاطاً دوسرے کوڈ بھی لکھ دیئے ہیں تاکہ کوئی نہ کوئی تو کام کرے۔

اور ایکسپائری مدت ختم ہونے سے پہلے آپ یہ کریں کہ Invite Friends پہ کلک کریں اور اس میں کوئی آپشن سیلیکٹ کریں، جیسے فیس بک پھر آپ کو کوئی کوڈ دیگا یا پھر کوئی لنک ملیگا، وہ آپ نے کسی دوست سے یا خود دوسرے ڈیوائس سے فریڈوم ڈاونلوڈ کر کہ وہ کوڈ لگانا ہوگا، جو وہ کوڈ لگائیگا اس کے 30 دن اور آپ کے 90 دن اور بڑھ جائینگے ایکس پائری ہے۔

چلانے کا طریقہ:

اسے On کرنے کیلئے Off پہ کلک کریں جب On نظر آئے تو یہ چل رہا ہے۔ لوکیشن تبدیل کرنے کیلئے لوکیشن پہ کلک کر کہ کوئی سا لوکیشن سیلکٹ کر سکتے ہیں، بہتر یہی ہے کہ بار بار تبدیل کریں۔ بس فیسبوک کیلئے ایک ہی ملک کا استعمال کریں کیونکہ اس سے آپ کا آکاونٹ بند ہو سکتا ہے۔

نوٹ: یہ سافٹویئر جو لاگز دکھاتی ہے مثلاً کہ اتنا ڈیٹا انکرپٹ کیا ہے، اتنے ویب سائٹ بلاک کئے ہیں، اتنے ٹریکنگ حملے روکے ہیں، یہ سب غلط دکھاتی ہیں اس لئے ڈرنے کی ضرورت نہیں کہ کوئی آپ پہ اتنے ٹریکنگ کرنا چاہ رہا ہے، اور یہ ٹریکنگ بھی اکثر ایڈز کے ذریعے سے ہی ہوتے ہیں۔

کوئی بڑی فائل ڈاونلوڈ کرنے کیلئے اس کا استعمال کیا کریں اگر ٹور سے ڈاونلوڈ نہ کر سکیں۔

اگر یہ ہر طریقے سے ایکسپائر ہو جائے تو آپ Hotspot shield کا elite ورشن ڈاونلوڈ کریں ٹورنٹ سے، وہ بھی گزارا کریگا عام براوزنگ اور ڈاونلوڈ کرنے کیلئے۔

Antivirus

اپنے کمپیوٹر میں اینٹی وائرس ضرور ڈالیں۔ایک اچھے اینٹی وائرس کا انتخاب آپ کو 80%ہیکنگ سے محفوظ رکھتا ہے۔ہیکنگ اور ہیکنگ سے بچنے کے بارے میں آگے بتائینگے ان شاءاللہ۔

سب سے بہترین اینٹی وائرس Bitdefender ہے۔اس کو آپ Torrent سے ڈاونلوڈ کر سکتے ہیں۔ٹوٹل سیکیورٹی ڈاونلوڈ کریں۔کیونکہ اس کا فری ورشن 15 یا 30 دن کیلیئے ہوتا ہے،ٹورنٹ سے آپ کو اس کا کریک ورشن ملیگا۔ایک لنک یہ ہے:

https://kat.cr/bitdefender-total-security-2015-build-18-21-0-1497-x86-x64-incl-trial-reset-keys-b-tman-t10267276.html

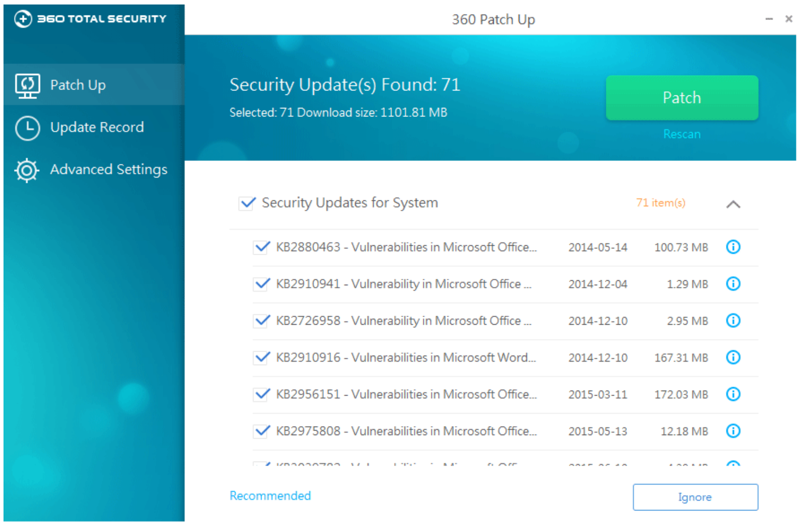
اس میں جونسا ورشن آپ ڈاونلوڈ کرنا چاہتے ہیں وہ سیلکٹ کریں یعنی 32bit یا 64bit ،اس میں دونوں موجود ہیں آپ ان میں سے ایک کو سیلیکٹ کریں ڈاونلوڈ کرنے کیلیئے جونسا آپ کا وینڈوز ہو۔ہر ایک 300mb ہے۔اس میں انسٹال نوٹس کو پڑھ کر انسٹال کریں۔

سست کمپیوٹر والوں کیلئے متبادل:اگر آپ کا سیسٹم سست ہے اور ایسا اینٹی وائرس برداشت نہیں کر سکتا تو آپ Qihoo 360 Total Security ڈاونلوڈ کر کہ انسٹال کریں۔یہ بہت ہلکا ہے اور سیکیورٹی بھی اچھی ہے۔اس کو آپ یہاں سے ڈاونلوڈ کر سکتے ہیں۔

http://www.360totalsecurity.com/en/download-free-antivirus/360-total-security/?offline=1

اس کو ڈاونلوڈ کر کہ انسٹال کریں۔اس کا اپڈیٹ ہونے کا طریقہ یہ ہے کہ یہ آپ کے سیسٹم کو اسکین کر کہ دیکھے گا کہ کون کون سے سافٹویئر انسٹال ہیں اور ان سافٹویئر کیلئے کون سے ضروری فائل انسٹال کرنے ہونگے۔

اس کا طریقہ یہ ہے کہ آپ اسے کھولیں،اس میں آپ Tool Box کو کھولیں پھر اس میں Patch Up پہ کلک کریں۔اسکین کر کہ آپ کو اس طرح کا لسٹ آئیگا۔



اگر آپ سب کو ایک ساتھ ڈاونلوڈ نہیں کر سکتے تو آپ ایک ایک کو سیلکٹ کر کہ بھی کر سکتے ہیں،بس جس کو ڈاونلوڈ کرنا ہے اسے سیلکٹ کریں اور Patch پہ کلک کریں۔

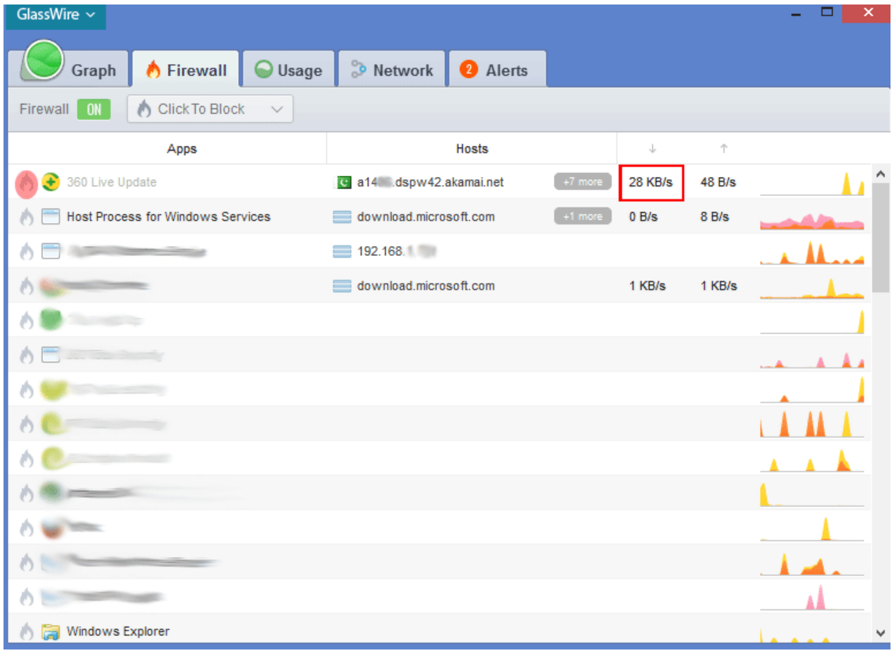
نوٹ: یہاں بھی وہی سوال پیدا ہو سکتا ہے کہ باقی اینٹی وائرس تو مفت نہیں ملتے یہ کیوں مفت ہے،تو یہ بتاتا چلوں کہ یہ سافٹویئر چائنا کی کمپنی Qihoo کی ہے،اور چائینا والے کمپنیوں کا مقصد یہ ہے کہ دوسرے امریکی کمپنیوں کا مقابلہ کرنے کے لئے لوگوں کو مفت سروس فراہم کرو۔اور شاید آگے جا کر جب مارکیٹ میں نام کما لیں اور جگہ حاصل کر لیں پھر اسی کا Pro ورشن متعارف کروائیں۔

اینٹی وائرس جونسا بھی ڈالیں پہلے فُل سیسٹم اسکین کریں۔اینٹی وائرس کو اپڈیٹ کرتے رہیں۔

فائروال/Firewall

فائروال ایک ایسا سافٹویئر ہے جس سے آپ دوسرے سافٹویئر کو انٹرنیٹ استعمال کرنے کی اجازت اور منع کر سکتے ہیں،اور انٹرنیٹ ٹریفک کی مکمل نگرانی کر سکتے ہیں۔اس سے آپ جاسوسی سافٹویئر کو بھی دیکھ سکتے ہیں،آگے بتائنگے کہ کیسے۔

بہتر یہ ہے کہ آپ اسی 360 Total Security کا فائروال ڈاونلوڈ کریں۔اس کیلئے آپ وہ اینٹی وائرس کھولیں اور اس میں Tool Box پہ کلک کریں،پھر اس میں Firewall پہ کلک کریں،وہ بیک گراونڈ میں ڈاونلوڈ ہو کہ انسٹال ہوگا۔اس کے فائروال کا نام Glasswire ہے۔اب آپ اسے کھولیں



Firewallوالے ٹیب کو کھولیں،اس میں سافٹوئیر کی لسٹ ہو گی جو انٹرنیٹ استعمال کر رہے ہیں،آپ جس کو چاہیں انٹرنیٹ استعمال کرنے سے منع کر سکتے ہیں اس کیلئے اس سافٹوئیر کے سامنے آگ والے نشان کو کلک کریں جیسا تصویر میں دکھایا ہے۔اور یہ بھی دیکھ سکتے ہیں کہ کونسی آئی پی استعمال ہو رہی ہے، جیسا اس تصویر میں پاکستان کے جھنڈے کا نشان ہے یعنی پاکستان کی آئی پی ایڈریس استعمال ہو رہی ہے۔اور کونسا سافٹوئیر کتنا ڈیٹا استعمال کر رہا ہے یہ بھی آپ دیکھ سکتے ہیں۔

اور کس سافٹوئیر نے کتنا ڈیٹا استعمال کیا ہے وہ دیکھنے کیلئے آپUsageوالے ٹیب پہ کلک کریں اور دیکھیں۔

جاسوسی سافٹوئیر کا اس طرح پتا چلے گا کہ وہ یہاں ڈیٹا استعمال کر رہا ہوگا،آپ دیکھیں کہ جس سافٹوئیر کو آپ نہیں جانتے اور وہ ونڈوز کا بھی نہیں ہے تو ممکن ہے کہ وہ جاسوسی سافٹوئیر ہو، مگر ایسے کمزور جاسوسی سافٹوئیر کو یہ اینٹی وائرس خود ہی سراغ لگا لگا۔۔۔

نوٹ: یہ اتنا اہم نہیں ہے، اگر کسی کا کمپیوٹر سست ہے تو وہ یہ نہ ڈالے۔ویسے تو ونڈوز کا اپنا فائروال بھی ہوتا ہے اور دوسرے بڑے اینٹی وائرس میں یہ چیز موجود ہے۔ضروری نہیں کہ صرف یہی ڈاونلوڈ کریں۔

مزید خفیہ رہنے اور انٹرنیٹ کی مکمل ٹریفک کو انکرپٹ اور ٹور کے ذریعے چلانے کیلئے TAILS کا استعمال

مختصر تعارف: TAILS ایک لینکس/Linux آپریٹنگ سسٹم ہے جس کا مقصد صارفین کی معلومات اور ڈیٹا وغیرہ کو خفیہ رکھنا ہے اور اس کے ذریعے جب آپ انٹرنیٹ استعمال کرینگے تو آپ کی مکمل ٹریفک ٹور/ Tor کے ذریعے چلے گی یعنی انکرپٹڈ ہوگی اور آئی پی ایڈریس بھی تبدیل ہوگی، اس کو آپ ٹور کا آپریٹنگ سسٹم بھی کہہ سکتے ہیں۔ چونکہ یہ لینکس آپریٹنگ سسٹم ہے اور جنہوں نے لینکس استعمال نہیں کیا ان کیلئے زیادہ فائدہ مند نہیں ہوگا، بس بنیادی سہولت حاصل کر سکینگے، جو اس میں پہلے سے موجود ہیں اور دیگر سافٹویئر انسٹال کرنے کیلئے لینکس کا استعمال سیکھنا ہوگا۔ اور جنہوں نے لینکس استعمال کیا ہے اور اس میں تھوڑی بہت مہارت رکھتے ہیں اُن کیلئے انتہائی مفید ثابت ہو سکتی ہے۔ TAILS کو USB میں ڈالنا ہوگا، یعنی TAILS چلانے کیلئے آپ کے پاس کم از کم USB 4 Gb ہونا ضروری ہے۔ یو ایس بی کو بوٹ ایبل بنانا ہوگا جس کا طریقہ آگے بتائینگے۔

TAILS کو یہاں سے ڈاونلوڈ کریں

https://tails.boum.org

اس لنک پہ جاکہ ایک طرف ڈاونلوڈ کا نشان ہوگا، اسے ڈاونلوڈ کریں، تقریباً 1Gb اس کا سائز ہے۔

USB کو بوٹ ایبل/ Bootable بنانے کیلئے آپ یہ سافٹویئر ڈاونلوڈ کریں

https://rufus.akeo.ie/

اس لنک پہ جائیں اور نیا ورژن ڈاونلوڈ کریں

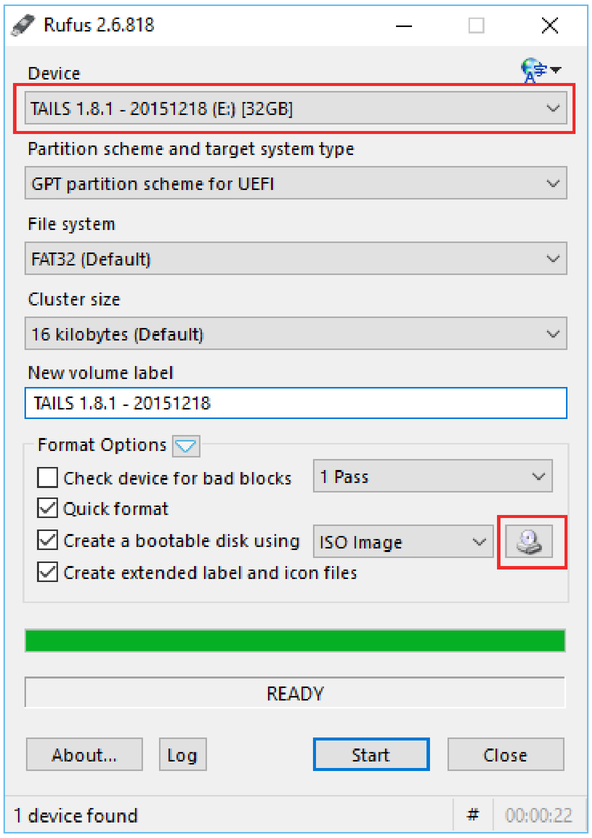
اس کے بعد اب یو ایس بی ڈالیں، اور Rufus سافٹویئر کو کھولیں۔

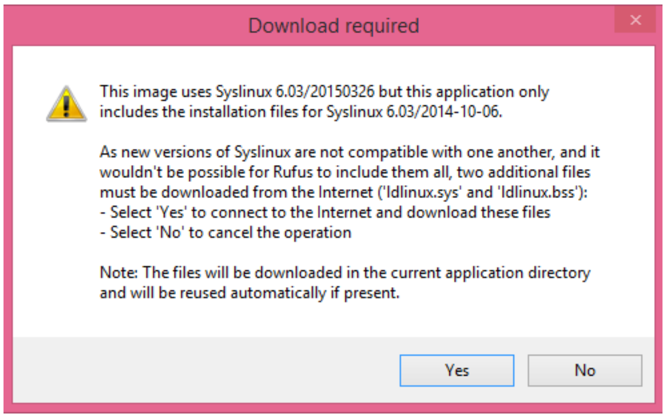
اب اس میں Device والے خانے میں اپنے یو ایس بی کا ڈرائیو سیلکٹ کریں۔

پھر نیچے سی ڈی کے نشان پہ کلک کریں جیسا اس تصویر میں دکھایا ہے۔

اس کو کلک کرنے سے ایک ٹیب کھلیگی اس میں TAILS والے فائل کو سیلکٹ کریں، جو آپ نے ڈاونلوڈ کیا تھا۔

اور پھر Start پہ کلک کریں۔ شاید آپ کے ہاں یہ ایرر آجائے۔





اس میں Yes پہ کلک کریں

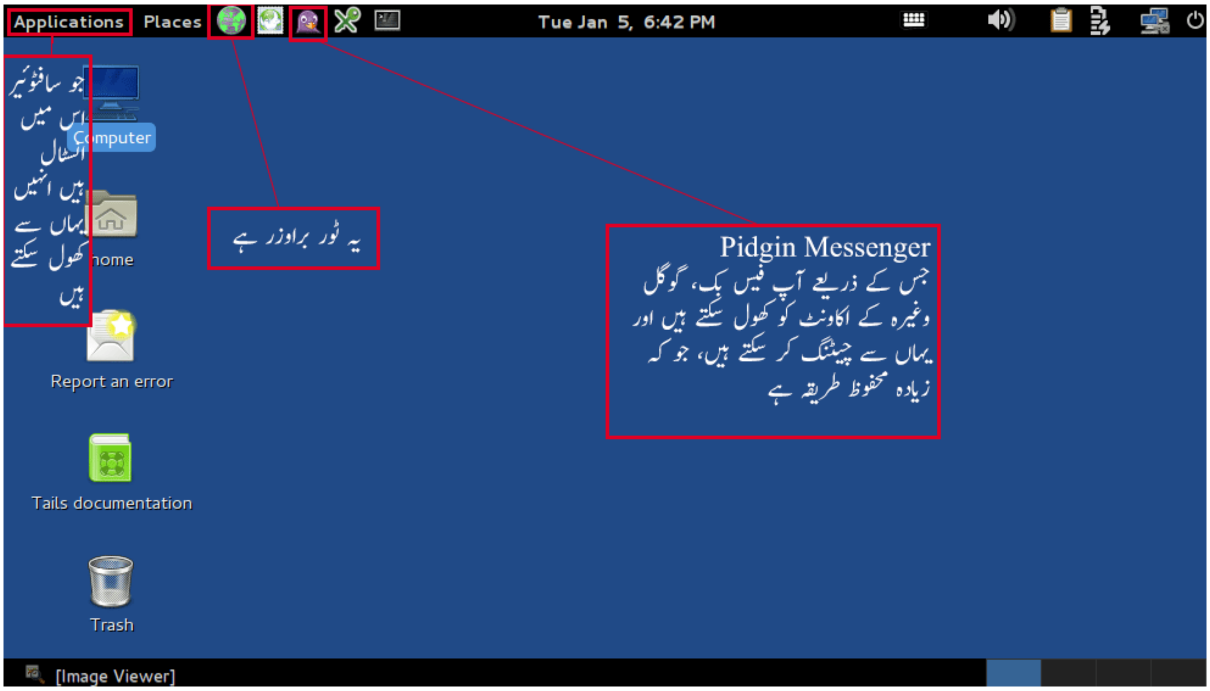
اس کیلئے آپ کو ایک منٹ کیلئے انٹرنیٹ چاہئے ہو گا کہ ایک ۵۰ کے بی کا فائل ڈاونلوڈ ہو گا۔ پھر فارمیٹ والے آپشن کو Ok کریں۔

بس پھر ایک دومنٹ میں وہ TAILS والی فائل اِس یوایس میں آجائیگی اور بوٹ ایبل بن جائیگی۔

پھر اس کو چلانے کیلئے اپنے کمپیوٹر کو ری اسٹارٹ کر کہ بائیوز سیٹ اَپ پہ جائیں اور وہاں فرسٹ بوٹ ڈیوائس کو USB کو سیلکٹ کر کہ سیو کریں اور کمپیوٹر ری اسٹارٹ کریں اور پھر اسی TAILS آپریٹنگ سیسٹم سے آپ کا کمپیوٹر اسٹارٹ ہو گا، شروع میں اگر دو آپشن آئیں تو Live والے کو سیلکٹ کریں۔

پھر ایک لاگ اِن کی اسکرین آئیگی اسے لاگ اِن کریں

پھر آپ کا TAILS آپریٹنگ سیسٹم کھل جایئگا، جو اس طرح کا ہو گا



ضروری چیزیں تصویر میں لکھ دی ہیں، اس میں بنیادی سافٹویر تو پہلے سے انسٹال ہیں مثلاً ویڈیو چلانے کیلئے اور اس طرح کے دوسرے بنیادی سافٹویر۔ باقی اس میں دیگر ضروری سافٹویر انسٹال کرنے کا طریقہ ان شاءاللہ پھر بتائینگے اگر زندگی رہی۔

TAILS کے فوائد:

- اس کو استعمال کرنے سے آپ کا ہارڈ سک پاسورڈ پہ رہیگا جس کو آپ استعمال تو کر سکتے ہیں مگر مناسب نہیں تاکہ بالفرض آپ کو کوئی ہیک کرنا چاہے تو آپ کے ہارڈ سک تک رسائی حاصل نہ کر سکے۔
- ہیکرز اور حکومت آپ کی ذاتی معلومات حاصل نہیں کر سکتے یعنی آپ کونسا ڈیوائیس، ونڈوز وغیرہ استعمال کر رہے ہیں اور آپ کی لوکیشن بھی معلوم نہیں کر سکتا۔
- چونکہ ونڈوز میں کافی ایسے سافٹویر ہیں جو انٹرنیٹ سے کنیکٹ ہوتے ہیں اور جب آپ آئی پی ایڈریس تبدیل کرتے ہو تو ان کے پاس تو ریکارڈ ہو گا کہ یہ آپ نے ہی استعمال کیا ہے، تو آپ اس خطرے سے بھی محفوظ ہو نگے۔

- آپ کی مکمل انٹرنیٹ ٹریفک انکرپٹڈ ہو گی، جس سے دوسروں کو پتا نہیں چلے گا کہ آپ کیا کر رہے ہیں انٹرنیٹ پہ۔
- خاص طور پر اگر آپ کوئی جہادی ویب سائٹ چلا رہے ہیں یا فیس بک پہ کوئی جہادی پیج چلا رہے ہیں اور آپ کو ہیکنگ سے خطرہ ہو تو یہ استعمال کریں۔

نوٹ:

- آپ ہارڈ سک کے ڈرائیو نہ کھولیں تاکہ سیکیورٹی مزید سخت رہے، اس لئے آپ کو اگر کوئی چیز ضرورت ہو تو آپ ایک اضافی یو ایس بی میں ڈالیں اور اُسی سے استعمال کریں۔
- اس میں جب آپ کوئی سافٹوئیر انسٹال کرینگے یا پھر کوئی فائل ڈاونلوڈ کرینگے وہ صرف اُسی سیشن تک محدود رہیگا اُس کے بعد جب آپ ری اسٹارٹ کرینگے تو وہ ڈیلیٹ ہو جائینگے۔ یعنی جس یو ایس بی میں ٹیلز ہے اس میں جو کچھ بھی آپ محفوظ کرینگے وہ صرف اسی سیشن تک محفوظ رہیگا پھر خود بخود ڈیلیٹ ہو جائیگا۔

دیگر چند اہم احتیاطی تدابیر

۱۔**ای میل ایڈریس**: جہادی کاموں کیلئے گوگل، مائکروسافٹ(Hotmail, outlook, live)اور یاہو وغیرہ کے ای میل ایڈریس استعمال نہ کریں۔کوشش کریں کہ ای میل ایڈریس

https://app.tutanota.de

https://protonmail.com

https://www.hushmail.com

https://safe-mail.net

پہ بنائیں جو بقول اُن کے انکرپٹڈ ہوتے ہیں،اور کوشش کریں کہ ٹوٹاوٹا اور پروٹون میل میں ہی بنائیں جو زیادہ معتبر ہیں۔پروٹون میل میں اکاونٹ بنانے کا طریقہ یہ ہے کہ ایک ریکوسٹ بھیجنا ہوگا جو اسے ۳ مہینے کے درمیان میں بن جائیگی۔

۲۔کسی بھی اجنبی بندے کا میل آجائے اور اس میں کوئی ڈاونلوڈ کی چیز ہو تو اسے ہر گز ڈاونلوڈ نہ کریں،جب تک سامنے بندے سے صحیح تعارف نہیں ہوتا۔اسی طرح کوئی بھی لنک اگر بھیجا ہو وہ بھی نہ کھولیں۔

۳۔کوشش کریں جس کمپیوٹر سے انٹرنیٹ استعمال کررہے ہیں اس میں ضروری اور خفیہ موادنہ رکھیں،بلکہ ان کو ایسی جگہ رکھیں جہاں انٹرنیٹ استعمال نہیں ہوتا۔

۴۔کوشش کریں کہ کمپیوٹر میں کم سے کم سافٹویئر انسٹال کریں۔

۵۔کبھی بھی ایک نام استعمال نہ کریں بلکہ ہر جگہ دوسرا نام رکھیں،اسی طرح ہر اکاونٹ کا ایک ہی پاس ورڈ نہ رکھیں بلکہ مختلف اکاونٹ کے مختلف پاسورڈ رکھیں اور ان کو وقتاً فوقتاً کو بدلتے رہیں۔

۶۔جب آپ جہادی ویب سائٹ کھول رہے ہوں یا جہادی مواد دیکھ رہے ہوں تو اس وقت ٹورنٹ کو بند کیا کریں۔

۷۔اگر جس کمپیوٹر سے انٹرنیٹ استعمال کررہے ہیں اور اس میں خفیہ مواد بھی موجود ہیں تو اُن کو ایسا نام دیں جو مشکوک نہ ہو یعنی عام سا کوئی نام رکھیں۔

۸۔ٹیکنالوجی سے آگاہ رہیں،ٹیکنالوجی اور نئی ہیکنگ سے متعلق پڑھتے رہیں۔ہیکنگ سے متعلق خبریں پڑھنے کیلئے اس ویب سائٹ کو دیکھا کریں

http://thehackernews.com

سیکشن سوم۔۔۔۔۔۔۔۔۔۔

ہیکنگ اور ہیکنگ سے بچنے کیلئے احتیاطی تدابیر

آج کل ہیکنگ بہت عام ہو چکی ہے اور لوگ لاعلمی میں اس کا شکار ہو جاتے ہیں، تو میں نے یہ ضروری سمجھا کہ ہیکنگ کے حوالے سے امتِ مسلمہ کو بنیادی باتیں، اور ان سے بچنے کے طریقے بتائے جائیں، تا کہ وہ دشمن کے حملے سے بچنے کے کیلئے احتیاطی تدابیر اختیار کر کہ محفوظ رہیں۔

اس میں ہم زیادہ تفصیل میں نہیں جائینگے بس وہ طریقے بتائینگے، جو آج دشمن استعمال کر رہا ہے۔

اس میں سے سب سے پرانا طریقہ "phishing/فیشنگ" کا ہے، جو کہ 2005 سے 2008 میں ایک وقت اپنے عروج پہ تھا لیکن بعد میں جب لوگوں کو اس کے بارے میں پتا چلا تو یہ طریقہ ناکام ہوا اور اس کا استعمال بھی ختم ہو تا گیا۔

لیکن ہمارے ملک میں چونکہ انٹرنیٹ کا استعمال ابھی ان دو تین سال میں زیادہ ہونا شروع ہوا ہے، اور لوگ بھی نئے ہیں، اُن کو اس بارے میں معلومات نہیں ہیں، تو دشمن نے اس کا فائدہ اٹھا کر وہی پرانا طریقہ اختیار کیا ہے۔

ا۔ فیشنگ

اس کا مفہوم تو بہت وسیع ہے جس کا مطلب یہ ہے کہ سامنے والے بندے کی ذاتی معلومات حاصل کرنا مثلاً کریڈٹ کارڈ نمبر، پن نمبر، کسی بھی آئی ڈی کا نام اور پاسورڈ وغیرہ۔ مگر ہماری اِدھر موضوع، فی الحال صرف کلون فیشنگ ویب سائٹ ہے، جس کا مطلب یہ ہوتا ہے کہ حملہ کرنے والا آپ کی جس آئی ڈی، پاسورڈ حاصل کرنا چاہتا ہے مثلاً فیسبوک، جی میل، یاہو وغیرہ

اس کام کو انجام دینے کے لئے، دشمن بالکل اصل ویب سائٹ کی طرح کی، ایک اپنی بنائی ہوئی جعلی ویب سائٹ بناتا ہے، اور پھر، اس کا لنک آپ کو بھیج دیتا ہے، جس میں آپ سے یوزر نیم اور پاسورڈ مانگتا ہے، یعنی جب آپ اس لنک کو کھولیں گے تو بالکل ویسا ہی پیج کھل جائے گا، جیسا کہ اصل ویب سائٹ کا ہوتا ہے۔

آیئے ہم آپ کو آسان الفاظ میں سمجھاتے ہیں،

مثال کے طور پر فیس بک کو لیتے ہیں

جیسے عام طور پر آپ جب فیس بک کا اصل لنک یعنی

https://www.facebook.com

یا https://m.facebook.com

ڈال کر کھولتے ہیں، تو وہ وہاں آپ سے آپکا فیس بک کا یوزر نیم اور پاسورڈ مانگتا ہے، وہ آپ اس میں ڈالتے ہیں تو آپ کا اکاونٹ کھل جاتا ہے،

اب یہ دشمن، جو آپ کا اکاونٹ ہیک کرنا چاہتا ہے، وہ یہ کرتا ہے کہ فیس بک کا وہ سب سے پہلے پیج، جس میں یوزر نیم اور پاسورڈ مانگا جاتا ہے، بالکل ہو بہو، ویسا ہی اسی طرح کا وہ ، اپنا ایک جعلی پیج بناتا ہے، اور اسے ایک لنک کی صورت میں آپ کو بھیجتا ہے، کہ یہ میرے پیج کا لنک ہے، اسے لائک کریں، جب آپ اس لنک کو کھولتے ہیں، تو کیا ہوتا ہے کہ، جیسا کہ فیس بک کے سب سے پہلے والا اصلی پیج، جس میں آپ سے یوزر نیم اور پاسورڈ مانگا جاتا ہے، بالکل اسی کی طرح کا، ہو بہو، پیج کھلتا ہے، جو دیکھنے میں اصل کی طرح ہی ہوتا ہے، لیکن حقیقت میں جعلی ہوتا ہے، جو دشمن کا بنایا ہوا ہوتا ہے، جو آپ سے آپ کا یوزر نیم اور پاسورڈ مانگتا ہے۔

اس جعلی پیج کو وہ اصل کے جیسا، وہ اس لئے بناتا ہے تاکہ جب آپ اسے کھولیں، تو آپ اسے فیس بک کا اصل پیج سمجھیں اور اپنا آئی ڈی اور پاسورڈ اس میں ڈال دیں۔ جب آپ اس میں اپنا آئی ڈی اور پاسورڈ ڈالیں گے، تو آپ کا آئی ڈی اور پاسورڈ، خود بخود اُس دشمن کے پاس چلا جاتا ہے، اور پھر، یا تو وہ آپ اکاونٹ کا پاسورڈ، خود تبدیل کر کہ کوئی دوسرا پاسورڈ ڈال کر آپ کے اکاونٹ پر مکمل قبضہ کر لیتا ہے، یا پھر پاسورڈ تبدیل نہیں کرتا، بلکہ ویسے ہی رہنے دیتا ہے، تاکہ آپ کو شک نہ ہو اور مطمئن رہیں، اور اپنے اکاونٹ کو عام روٹین کے مطابق استعمال کرتے رہیں، اور دشمن اسی آپ کے یوزر نیم اور پاسورڈ کو استعمال کرتے ہوئے، آپ کے اکاونٹ کی جاسوسی کرتا رہتا ہے کہ آپ کس کس سے کیا بات کرتے ہیں۔

مگر یہ کرنے سے پہلے وہ ایک لمبے عمل سے گزرتا ہے، مثلاً شروع میں آپ سے دوستی کرتا ہے، اپنے کو مجاہد ظاہر کرتا ہے یا جس بھی فیلڈ میں آپ کی رجحان ہو، اسی مطابق بات کر کہ آپ سے دوستی کرتا ہے تاکہ جب آپ کو وہ یہ لنک بھیج دے تو آپ اسے کھولیں اور اس پہ شک نہ کریں اور اگر فیس بک اکاونٹ ہو تو یہ کہہ کر دھوکہ دینا چاہے گا، کہ یہ میرا پیج ہے، اسے لائک کر دیا اس طرح کا دوسرا ڈرامہ بناتا ہے۔

اس سے بچنے کا طریقہ:۔۔۔۔۔۔ اس سے بچنا تو بہت آسان ہے بس یہ دیکھیں کہ آپ نے جس لنک کو کھولا ہے جو آئی ڈی پاسورڈ مانگ رہا ہے، کیا وہ واقعی فیسبوک کی اپنی اصل سائٹ ہے یا نہیں، یعنی وہ اس طرح نیچے دیئے گئے دو لنکس کی طرح ہوں۔ ان دونوں لنکس میں، پہلا لنک فیس بک کا کمپیوٹر صارفین کے لئے، اور دوسرا موبائل صارفین کے لئے ہے

https://www.facebook.com

یا https://m.facebook.com

اگر اوپر دیئے گئے ان دونوں کے علاوہ کوئی لنک ہو تو آپ سمجھ جائیں کہ یہ فیشنگ سائٹ ہے۔

فیشنگ سائٹس کس طرح کی ہوتی ہیں:۔۔۔۔۔۔

ایجنسی والوں کا ایک مشہور فیشنگ ویب سائٹ یہ ہے جس سے وہ مجاہدین کو دھوکہ دینا چاہ رہے ہیں:

http://talibislam.somee.com/?fbid=934448985285672886 11&set=a.763335483356816.08379.98 1729056298491&type=1&relevant_count=1&ref=nf

اصل لنک یہ:

http://talibislam.somee.com

ہے، آپ کو دھوکہ دینے کیلئے آگے اتنا بڑا لنک ڈالا جاتا ہے کہ آپ اس پہ شک نہ کریں۔

تو اس میں آپ دیکھ سکتے ہیں کہ یہ فیسبوک کی ویب سائٹ نہیں ہے، یہ ایک فیشنگ سائٹ ہے۔

اور کچھ ایسی بھی ہوتی ہیں

جو فیس بک کی طرح لکھائی میں ہوتے ہیں، یعنی فیس بک سے ملتا جلتا تلفظ ہوتا ہے۔

مثلاً یہ نیچے دو لنکس دیکھیں کہ ان کا تلفظ فیس بک سے ملتا جلتا ہے۔

www.fecebock9.tk

اور www.fasebo0k.wapka.me

یہ دو اور فیشنگ سائٹ ہیں جو دھوکہ دینے کیلئے فیسبوک کا نام بھی استعمال کر رہے ہیں، مگر غور سے دیکھیں تو آسانی سے معلوم ہو گا کہ یہ فیسبوک کی سائٹ نہیں ہیں۔

اس لئے نقالوں سے ہوشیار!!!!

تو آپ الفاظ کو صحیح دیکھیں اور ایسی سائٹ آئے تو کبھی لاگ اِن نہ کریں۔ یا چیک کرنے کیلئے غلط آئی ڈی اور پاسورڈ لگائیں اور دیکھے کیا ہوتا ہے، عموماً یہ ہوتا ہے کہ دوسرا ایک پیج کھلتا ہے یا فیسبُک کا اصل لاگ اِن پیج کھلتا ہے یا کچھ اور بھی ترتیب وہ کرتا ہے۔

۔۔۔۔۔۔۔۔اگر آپ اس مسئلے کا ماضی میں شکار ہو چکے ہیں، تو فوراً اپنے اکاونٹ کا پاسورڈ تبدیل کریں۔۔۔۔۔۔۔۔

آج کل فیشنگ سائٹ کا بنانا بہت آسان ہے، یہ کسی بھی ہیکنگ فورم سے آسانی سے فائل مل جاتے ہیں، ان کو بس کسی مفت ویب ہوسٹنگ پہ اپلوڈ کیا جاتا ہے اور اسکا لنک لوگوں کو دیا جاتا ہے جو بھی اس سے لاگ اِن ہوگا، اس کا یوزر نیم اور پاسورڈ چلا جائے گا۔ اس لئے اس کے بھیجنے والے کو ہیکر مت سمجھیں، اور نہ ان سے گھبرانے کی ضرورت ہے، یہ ایک انتہائی درجے کی ناکام کوشش ہے، جو انہوں نے اپنائی ہے، لیکن لوگ لاعلمی کی وجہ سے اس کا شکار ہو جاتے ہیں۔

۲۔RATs (remote administrative tools)

یہ ایک قسم کا ٹروجن/سپائی ویئر (جاسوسی سافٹوئیر) ہے یا عام سادہ زبان میں وائرس بھی کہہ سکتے ہیں۔ یہ ایک ایسا جاسوسی سافٹوئیر ہے جس میں حملہ کرنے والا اس کو آپ کے کمپیوٹر میں بھیج کر آپ کی کمپیوٹر کو استعمال کر سکتا ہے، یعنی اس میں آپ کی فائلز وغیرہ کو دیکھ سکتا ہے آپ کے لیپ ٹاپ کے کیمرے کو کھول سکتا ہے یعنی آپ کے کمپیوٹر سے کچھ بھی کر سکتا ہے اور آپ کو بالکل معلوم بھی نہیں ہوگا۔ اور ان میں ہزاروں فنکشن ہوتے ہیں ممکن ہے جس وقت آپ نیٹ استعمال کر رہے ہیں اس وقت وہ استعمال نہیں کر رہا ہوتا، اور جس وقت وہ استعمال کر رہا ہوتا ہے اس وقت آپ استعمال نہیں کر رہے ہوتے تو وہ اس سافٹوئیر کے مختلف آپشن کو سیلیکٹ کر سکتا ہے مثلاً اس آپشن پہ رکھتا ہے کہ آپ کے کمپیوٹر کی اسکرین شاٹ ہر ۱۰ امنٹ بعد لیتا رہے اور جب نیٹ موجود ہو تو اس وقت اس بندے پہ بھیج دے، اور بھی کئی ایسے فنکشن کے ساتھ یہ سافٹوئیر آتے ہیں۔ مگر یہ خود بخود نہیں آتے اِن کو حملہ کرنے والا آپ کی کمپیوٹر تک کسی نہ کسی ذریعے سے پہنچاتا ہے اور انسٹال کرواتا ہے۔ اور یہ طریقے مختلف ہو سکتے ہیں، مثلاً USB میں ڈال کر اور یو ایس بی کو آٹورن پہ رکھا ہو یعنی جیسے ہی آپ اس کی دی ہوئی یو ایس بی ڈالینگے فوراً سے یہ سافٹوئیر انسٹال ہو گی اور خفیہ طور پر چل رہا ہوگا، دوسرا طریقہ وہ یہ کہ وہ آپ کو کوئی لنک بھیجے گا کہ اس لنک میں بہت اہم معلومات ہیں جب آپ اس کو ڈاونلوڈ کر کہ اس پہ کلک کرینگے تو یہ سافٹوئیر انسٹال ہو جائے گا اور خفیہ طور پر چل رہا ہوگا، اور اس کو بھیجنے کے وہ مختلف حیلے نکال سکتا ہے، مقصد اس کا آپ سے اس کو کلک کروانا ہی ہے چاہے جو نسا بھی طریقہ استعمال کرے۔ ویسے بازار میں سی ڈی اور ڈی وی ڈی میں بھی ان کو ڈال سکتے ہیں اور اکثر ایسا ہوتا بھی ہے کہ سی ڈیز میں ایسے سافٹوئیر پائے گئے ہیں۔

یہ صرف کمپیوٹر نہیں بلکہ اینڈرائڈ موبائل کے لئے بھی ایسے سافٹوئر آئے ہیں جن میں موبائل کی جاسوسی کی جاسکتی ہے، موبائل کے میسجز، واٹس ایپ وغیرہ کے میسیجز، کال سننا، کنٹیکٹس دیکھنا وغیرہ اس میں ممکن ہے۔ اور اس کا بھیجنے کا طریقہ بالکل مختلف ہے کمپیوٹر والے سے، اس میں حملہ کرنے والا آپ کو کوئی گیم یا ایپ کا لنک بھیجے گا یا ویسے آپ کو دیگا اگر آپ کا کوئی اپنا ہو، اور اسی گیم یا ایپ کے ساتھ وہ اپنا یہ جاسوسی سافٹوئیر ملاتا ہے اور جب آپ اس گیم کو انسٹال کرینگے تو یہ جاسوسی سافٹوئیر خود بخود انسٹال ہو گا۔

ریٹس سے بچنے کا طریقہ: کسی بھی سافٹوئیر کو بغیر جانے انسٹال نہ کریں۔

کسی بھی انجان بندے کے بھیجے ہوئے لنک کو کلک مت کریں۔

بازاری سی ڈیز اور ڈی وی ڈیز سے اجتناب کریں۔

اکثر سافٹوئیر کو ڈاونلوڈ کرنے کے لئے ایک دوسرے انسٹالر کو ڈانلوڈ کر کہ اس سے اس سافٹوئیر کو ڈاونلوڈ کیا جاتا ہے، ایسے انسٹالر سے اجتناب کریں۔

براوزر میں ایڈبلاک پلگ اِن ضرور ڈالیں۔

یو ایس بی آٹو پلے یا آٹورن کا آپشن بند کریں۔ **نوٹ:** اس کو بند کرنے کا طریقہ اس ٹٹوریل کے آخر میں بتایا ہے۔ وہاں ملاحظہ فرمائیں۔

آخری اور سب سے ضروری چیز ایک اچھا اینٹی وائرس ضرور ڈالیں۔ ہمارے مطابق بہترین اینٹی وائرس بٹ ڈیفینڈر ہے۔
مگر چونکہ ریٹس بھی اپڈیٹ ہوتے رہتے ہیں اور ان کو ایسا بنایا جاتا ہے کہ اینٹی وائرس اس کو نہ پکڑ سکیں۔ یہ ایک قسم کا مقابلہ ہے ٹروجن / ریٹس اور اینٹی وائرس کے درمیان کے وہ ایسا بناتے ہیں کہ اینٹی وائرس ان کو پکڑ نہ سکیں اور پھر اینٹی وائرس بھی اپڈیٹ ہوتے ہیں جن میں نئے ٹروجن اس میں پکڑے جا سکتے ہیں۔ آپ خبروں میں دیکھتے ہونگے کہ فلاں اینٹی وائرس نے ایسا ٹروجن پکڑا ہے جس سے لاکھوں کمپیوٹر متاثر ہوئے ہیں، اور یہ ٹروجن فلاں ملک سے پھیلا ہے۔ یعنی ایک ملک کے ہیکرز دوسرے ملک کی جاسوسی انہی سافٹویئر/ٹروجن/ریٹس سے کرتی ہے۔ اور وہ مکمل FUD یعنی فُلی اَن ڈیٹیکٹ ایبل یعنی اس کو کوئی بھی اینٹی وائرس نہیں پکڑ سکتی۔ مگر پھر کوئی نہ کوئی اینٹی وائرس جب اس کا سراغ لگاتی ہے تو وہ دوسرا بناتے ہیں۔ مگر یہ وہ ریٹس ہیں جو ایک ملک دوسرے ملک کی جاسوسی کیلئے بناتا ہے۔ باقی جو عام ریٹس ہیکرز نے عوام کیلئے بنائی ہیں ان کو یہ اینٹی وائرس پکڑتے ہیں، مگر وہ دوسرا نیا ورشن بناتے ہیں اس طرح یہ سلسلہ جاری ہے۔

اور اینڈرائیڈ موبائل والے اس طرح اس سے بچ سکتے ہیں کہ کسی بھی اجنبی سے کوئی گیم وغیرہ نہ لیں۔
ویسے تو اس کا ایک ہی حل یہی ہے کہ آپ صرف اور صرف گوگل پلے اسٹور سے چیزیں ڈاونلوڈ کریں باقی کسی بھی جگہ سے ڈاونلوڈ کرنے سے شبہ ہے کہ اس میں کوئی دوسرے ملک والے نے اس میں ڈال کر بھیجا ہو۔ گوگل پلے اسٹور مکمل سیکیور ہیں۔
دوسرا آپ اچھا سا اینٹی وائرس بھی ڈالیں۔
ایک بات اس ضمن میں یہ بھی بتانا چاہونگا جو پہلے بھی کہی تھی کہ جو ایپ یا گیم آپ ڈالتے ہیں تو اس میں وہ مختلف پرمیشن مانگتا ہے، جس میں آپ کے میسیجز، کنٹیکٹس، لوکیشن وغیرہ شامل ہوتے ہیں، حالانکہ گیم کیلئے ان پرمیشن کا کوئی سروکار ہی نہیں۔ اصل میں ہوتا یہ ہے کہ ان گیمز میں ایڈز ہوتے ہیں جو ان گیم کے کمپنی کو پیسے دیتے ہیں اور یہ گیمز ان ایڈورٹائزمنٹ والے کو ان کے ڈیٹا فراہم کرتے ہیں۔ یعنی یہ گیم آپ کیلئے مفت ہے مگر اس کے بدلے میں وہ آپ ہی کا سودا کر رہا ہوتا ہے، ضروری نہیں کہ سب ایسا کرتے ہیں لیکن کچھ ایسا کرتے ہیں۔
جیسا حال ہی میں خبر آئی تھی کہ AVG اینٹی وائرس اپنے صارفین کی ڈیٹا حاصل کر کہ اپنے ایڈز/ایڈورٹائزمنٹ والے کمپنیوں کو بیچتی ہے۔ اور یہی بات تنبیہ کہ طور پر لکھی تھی کہ کسی بھی چیز کو مفت نہ سمجھیں، ہر وقت تحقیق کریں کہ یہ اگر مجھے یہ سروس مفت میں دے رہا ہے اس کے پیچھے کیا راز ہے، کہیں ایسا تو نہیں کہ مفت کے چکر میں اپنا سودا تو نہیں کر رہا ہوں۔

تو ایسے گیمز اور ایپس سے بھی احتیاط کریں اگر آپ نے ایپ پرمیشن کو ختم نہیں کیا یا آپ کے موبائل میں پرمیشن ختم نہیں ہو رہے۔

عام مشہور ریٹس یہ ہیں:

Xtreme Rat

DarkComet

CometRat

NJ rat

Pandroa rat

CyberGate

BlackShades

Novalite

اور اینڈرائڈ کافی الحال ایک ہی ریٹ زیادہ مشہور ہے

Droid jack

اور حال ہی میں ایک خبر آئی تھی کہ پاکستانی حکومت نے ایک دوسرے ملک کے ہیکنگ ٹیم سے اس طرح کا ایک ریٹ/ٹروجن بنوایا ہے اور کروڑوں روپے میں اس کو خریدا ہے۔
اس لئے اب ہمیں محتاط ہونا ہوگا ظاہر سی بات ہے اس نے یہ اینڈیا کی جاسوسی کے لئے تو نہیں بلکہ اپنے عوام ہی کی جاسوسی کیلئے خریدا ہے۔

USB،CDs،یا دیگر میموری کارڈ وغیرہ کے آٹو پلے کو بند کرنے کا طریقہ: چونکہ ہر ونڈوز میں اُس کا طریقہ مختلف ہے اس لئے ہم یہاں ایسا طریقہ بتائینگے جو ونڈوز 98 سے لیکر ونڈوز 10 تک کام کرے۔اور وہ ریجسٹری میں تبدیلی سے ہوتا ہے۔اس کیلئے:

۱۔سب سے پہلے Start پہ کلک کریں اور وہاں Run پہ کلک کریں،ونڈوز 8 اور اس سے اوپر والے Start پہ کلک کریں یعنی ونڈوز کے نشان پہ کلک کریں چاہے کمپیوٹر میں یا کی بورڈ میں، پھر اس میں سرچ پہ کلک کریں۔

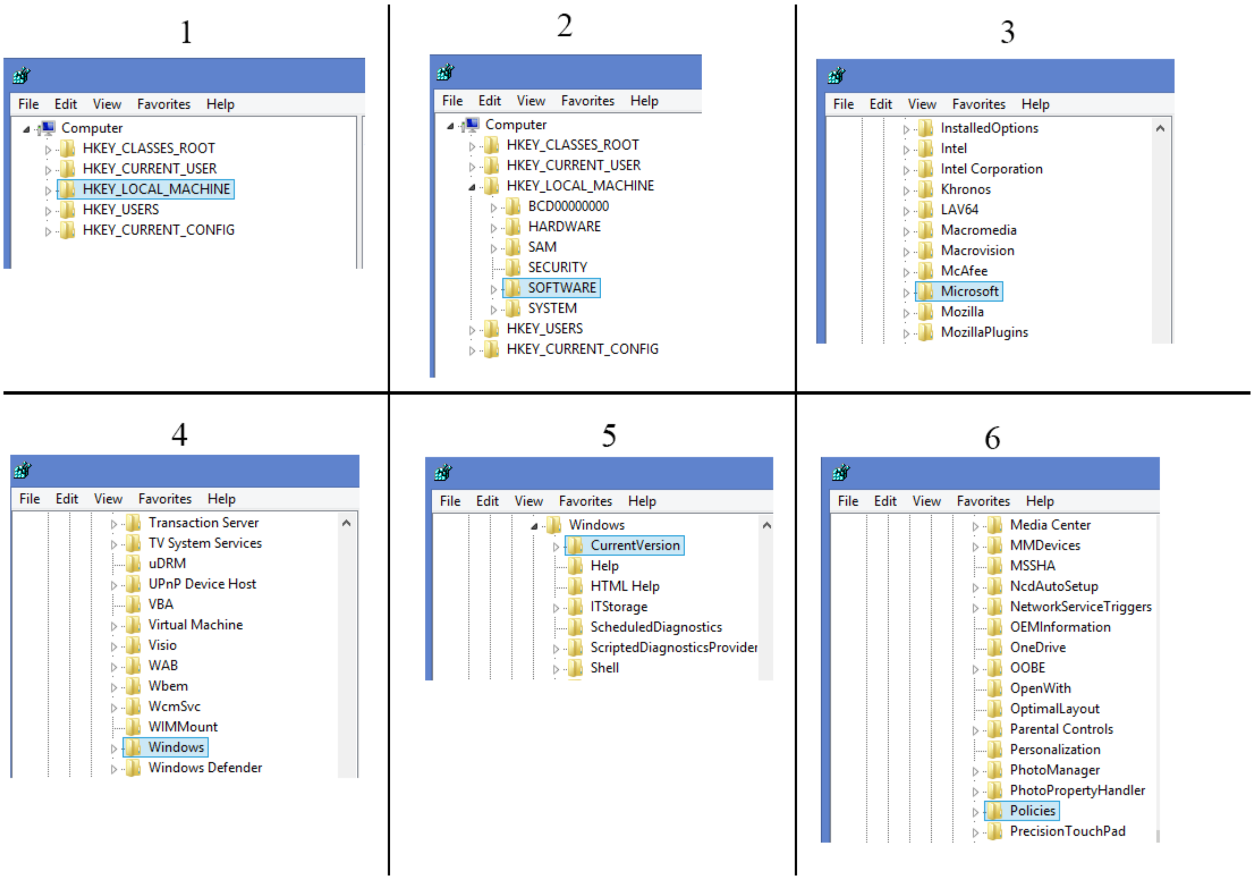
۲۔اب رَن یا سرچ میں regedit لکھیں اور اس نام والے کو کھولیں۔

۳۔پھر اس میں HKEY_LOCAL_MACHINE پہ ڈبل کلک کریں۔

۴۔پھر اس فولڈر کے اندر Software کو ڈبل کلک کریں۔پھر اس میں Microsoft کو ڈبل کلک کریں۔پھر اس میں windows کو ڈبل کلک کریں۔پھر اس میں CurrentVersion کو ڈبل کلک کریں۔پھر اس میں policies پہ ڈبل کلک کریں۔جیسا نیچے تصویر میں دکھایا ہے۔

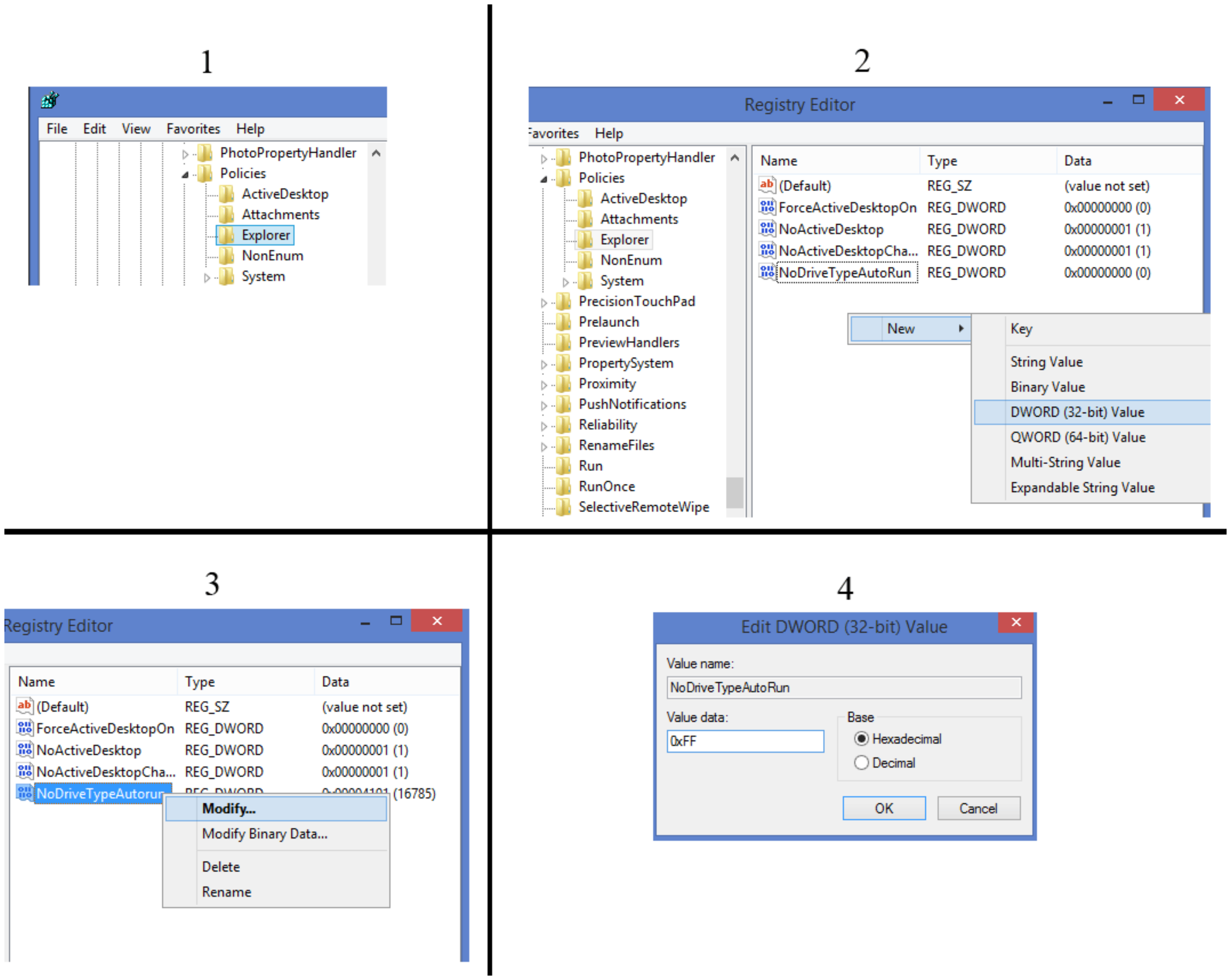
یعنی: HKEY_LOCAL_MACHINE

=>Software=>Microsoft=>windows=>CurrentVersion=>policies



۵۔پھر Policies میں Explorer پہ کلک کریں۔دائیں طرف اس کے ریجسٹری ظاہر ہونگے۔

۶۔اُس میں دیکھیں کہ NoDriveTypeAutoRun نامی ریجسٹری/فائل موجود ہے یا نہیں۔اگر نہیں ہے تو بنالیں۔اس کیلئے دائیں طرف والے خانے میں رائٹ کلک کریں اور new پہ جائیں اور اس میں DWORD پہ کلک کریں۔اور اس کو نام دیں NoDriveTypeAutoRun کا جیسا نیچے تصویر میں دکھایا ہے۔



۷۔اگر پہلے سے اس نام کا موجود ہے یا اب بنایا ہے دونوں صورتوں میں آپ اُس NoDriveTypeAutoRun پہ رائٹ کلک کریں اور Modify پہ کلک کریں۔

۸۔پھر اس کے value data میں 0xFF لکھیں اور Ok پہ کلک کریں۔

کمپیوٹر ری اسٹارٹ کریں، اب تمام ڈرائیو کے آٹورن / پلے بند ہو جائینگے۔

ونڈوز 8,8.1 وغیرہ میں اس کا آسان متبادل طریقہ:

آپ سیٹنگز میں جائیں، پھر Change PC Settings میں جائیں اور پھر PC and Devices اور پھر اس میں Autoplay اور اس کو Off کر دیں۔

نوٹ: پھر جب بھی یو ایس بی لگائیں تو اس کے ڈرائیو کو کبھی ڈبل کلک نہ کریں، بلکہ رائٹ کلک کر کہ اوپن کریں، کیونکہ اگر اس میں کوئی ٹروجن یا وائرس وغیرہ ہو تو ڈبل کلک سے بھی آٹورن ہو کہ انسٹال ہو گا۔

۳۔Keyloggers/کی لوگرز

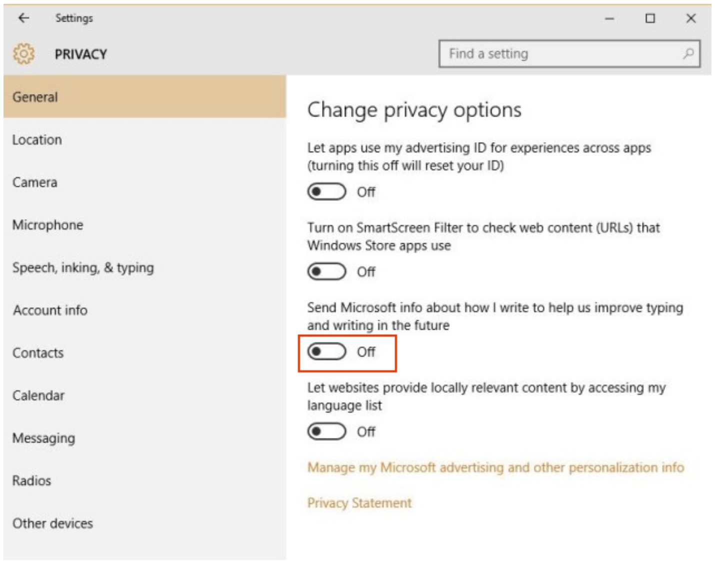
یہ بھی ایک قسم کا ریٹ/ٹروجن ہے، مگر اس کا کام صرف ایک ہے وہ یہ کہ یہ صرف آپ کے کی بورڈ کی جاسوسی کرتا ہے کہ آپ کیا کیا لکھ رہے ہیں، آپ کی تمام لکھائی کی جاسوسی کرتا ہے اور حملہ کرنے والے پہ بھیجتا ہے۔اور یہ بھی فنکشن ہے کہ ماوس کے پوائنٹر کی جاسوسی کرے یعنی جس چیز/فولڈر/فائل وغیرہ پر رکھتا ہے اس کا نام جائے۔آج کل نئے فنکشن کے ساتھ آرہے ہیں جس میں یہ ہوتا ہے کہ جب آپ فیس بک یا کوئی دوسرا اکاونٹ کھول رہے ہوں ان کی جاسوسی کرے وغیرہ۔یعنی کام پھر بھی وہی آپ کے ٹائپنگ کی جاسوسی ہی ہے۔یہ فنکشن دوسرے ریٹس میں بھی ہیں مگر چونکہ اس کی لوگر کا کام محدود ہے اور اپنے خاص کام کی وجہ سے اس کا الگ نام ہے اس لئے اس کو الگ لکھنا مناسب سمجھا۔باقی اس کے بھیجنے کا طریقہ اور بچنے کا طریقہ وہی ہیں جو اوپر بتا چکا ہوں۔

ونڈوز ۱۰ میں پہلے سے انسٹال شدہ کی لاگر کو نکالنے کا طریقہ: ونڈوز ۱۰ میں مائکروسافٹ کی طرف سے پہلے سے ایک کی لاگر انسٹال ہے جو آپ کے تمام لکھائی کی جاسوسی کرتا ہے اور اس کو مائکروسافٹ کی کمپنی پہ بھیجتا ہے۔اور یہ چھپکے سے نہیں کر رہا، بلکہ اُن کا کہنا ہے کہ اس سے صارفین کو مزید سہولت فراہم کرنا مقصود ہے اور جو اس کو بند کرنا چاہے اسے بند کر سکتا ہے۔(ہمیں تو کوئی سہولت اس میں دکھائی نہیں دی)۔خیر اس کو بند کرنے کا طریقہ یہ ہے:

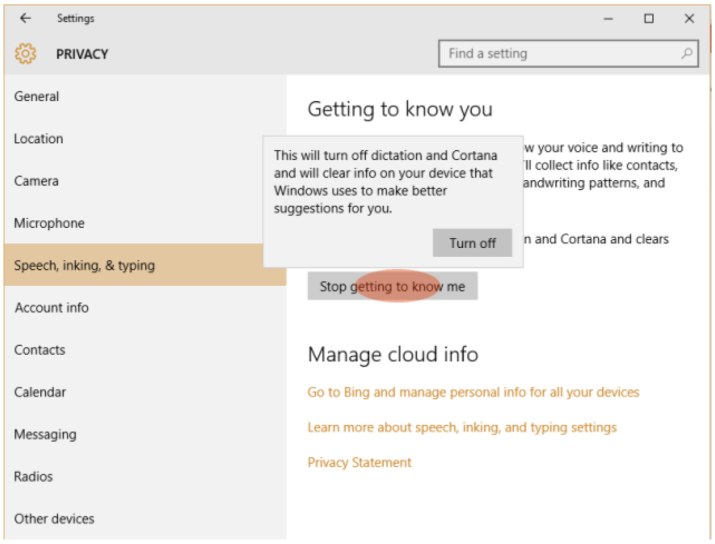
Start پہ کلک کریں، پھر Settings میں جائیں، پھر Privacy میں جائیں

پھر General میں send Microsoft info about how I write… کو Off کریں، جیسا اس تصویر میں دکھایا ہے۔

1

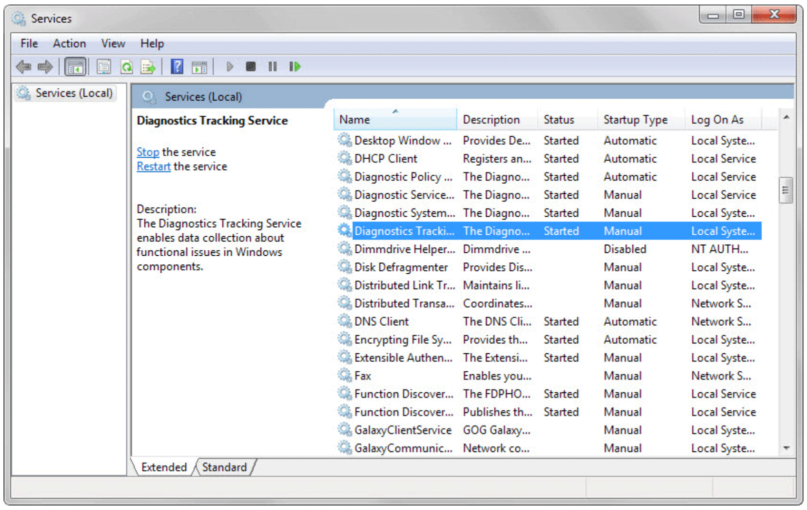


2



پھر Speech, inking & typing والے کیٹگری میں جائیں، اور اس میں Stop getting to know me پہ کلک کریں اور ایک اور اسکرین آئی گی اس میں Turn off پہ کلک کریں۔

اس کے علاوہ آپ کو ایک اور ٹریکنگ آپشن بند کرنا ہوگا، پہلے یہ دیکھیں کی وہ ٹریکنگ آپ کے ونڈوز میں موجود ہے یا نہیں، اس کیلئے ٹاسک مینیجر کو کھولیں، اُس میں Services پہ کلک کریں، پھر سروس میں نیچے ایک آپشن ہوگا Open Services کا اسے کلک کریں،



اب Diagnostics Tracking Service دیکھیں موجود ہے یا نہیں۔۔

اگر موجود ہے تو آپ اس کو یہاں سے stop کر سکتے ہیں۔

مگر یہ دوبارہ اسٹارٹ ہو جاتا ہے، اس لئے اس کو جڑ سے ختم کرنا لازمی ہے

اس کیلئے کمانڈ پرومپٹ/ڈوس/cmd/dos کھولیں۔ ڈوز کھولنے کیلئے سرچ پہ cmd لکھیں command prompt لکھا آئیگا اس کو رائٹ کلک کر کہ Run as administrator سے کھولیں۔ اب اس میں یہ چیز لکھیں

```
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>sc stop DiagTrack

SERVICE_NAME: DiagTrack
    TYPE           : 10  WIN32_OWN_PROCESS
    STATE          : 3  STOP_PENDING
                    (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
    WIN32_EXIT_CODE    : 0  (0x0)
    SERVICE_EXIT_CODE  : 0  (0x0)
    CHECKPOINT         : 0x3
    WAIT_HINT          : 0x0

C:\Windows\System32>sc delete DiagTrack
[SC] DeleteService SUCCESS

C:\Windows\System32>
```

sc stop DiagTrack

انٹر کریں، اس سے وہ بند ہو جائیگا، پھر یہ لکھیں

sc delete DiagTrack

انٹر کریں، اس سے یہ ڈیلیٹ ہو جائیگا۔

اب اِن سب کو کرنے سے اِن شاءاللہ مائکروسافٹ کے کی لاگر سے محفوظ ہونگے۔

۴۔ایکس ایس ایس ایکسپلا ئیٹیشن/ XSS Exploitation یا کراس سائٹ ایسکرپٹنگ/Cross-site Scripting

یہ ایک قسم کا حملہ ہے جس میں حملہ کرنے والا کسی ویب سائٹ کی کمزوری دیکھ کر اس میں اسکرپٹ / کوڈنگ کرتا ہے جس سے وہ اس ویب سائٹ دیکھنے والے لوگوں کی معلومات حاصل کرتا ہے،اور بعض اوقات کوئی پلگ اِن انسٹال کرواتا ہے کہ اس ویب سائیٹ کو کھولنے کے بعد آپ کو کوئی پلگ اِن انسٹال کرنے کا بتارہا ہوتا ہے مثال کے طور پر وہ یہ دکھاتا ہے کہ اس ویڈیو کو دیکھنے کیلئے فلیش پلئیر پلگ اِن ڈالیں اور یہاں کلک کریں انسٹال کرنے کیلئے، جب آپ اس کے پلگ اِن کو انسٹال کرتے ہیں تو وہ آپ کے براوزر سے کوکیز کو چراتا ہے یعنی آپ کے براوزر کے کوکیز اس حملہ کرنے والے کے پاس جائینگے، کوکیز میں آپ کے محفوظ کردہ پاسورڈ ہوتے ہیں جو آپ کسی اکاونٹ کو کھولنے کے بعد سیو پاسورڈ کرتے ہیں۔آج کل ہیکرز اس سے بھی ایک قدم آگے گئے ہیں یعنی وہ صرف کوکیز نہیں بلکہ آپ کے ڈیٹا تک رسائی حاصل کر سکتے ہیں۔اس حملے کی سب سے بڑی مثال فیس بک ہے، جس کا آگے آپ کو بتائینگے۔اگرچہ فیس بک نے کافی حد تک اس حملہ سے اپنے ویب سائٹ کو محفوظ بنایا ہے، مگر حملہ کرنے والا کسی دوسری جہادی ویب سائٹ کے کمزوری کو دیکھ کر یہ حملہ کر سکتا ہے،اس کی زندہ مثال عالمی اسلامی میڈیا محاذ کے ویب سائٹ پر یہ حملہ ہوا تھا یعنی gimf.com والا ویب سائٹ جس میں اسرار المجاہدین سافٹوئیر کا لنک موجود تھا، خیر بعد میں تو یہ ویب سائٹ مکمل ہیک ہوگئی تھی جب فرانس کی مبارک کاروائی ہوئی تھی، چارلی ہیبڈو خبیثوں نے اس ویب سائٹ کو مکمل ہیک کی تھی اور نازیبا کارٹون ڈالے تھے۔۔۔

اس سے بچنے کا طریقہ: جیسا پہلے بتا چکا ہوں کہ جب بھی آپ انٹرنیٹ استعمال کریں تو پرائیٹ ونڈو یا انکوگنیٹو ونڈو سے استعمال کریں جس میں کوکیز اور پاسورڈ محفوظ نہیں ہوتے اور سب سے بہتر طریقہ تو یہ ہے کہ ٹور براوز ہی استعمال کریں جس میں نہ کوکیز محفوظ ہوتے ہیں اور نہ ہی کوئی اسکرپٹ اس میں کام کرتی ہے، تو جب آپ ٹور استعمال کررہے ہوں تو کافی حد تک اس حملے سے محفوظ ہونگے۔

فیس بک پہ XSS و دیگر ہیکنگ سے بچانے کا طریقہ

اپیلی کیشن پرمیشن:۔۔۔۔

فیس بک پر آپ جب بھی کسی اپیلی کیشن، گیم، کویز وغیرہ کو استعمال کرنا چاہے تو اس پہ جانے سے پہلے آپ کو ایک اور صفحہ سے گزرنا پڑتا ہے جہاں اپیلی کیشن کی آپکے اکاؤنٹ تک رسائی سے متعلق معلومات لکھی ہوتی ہیں۔یعنی وہ اس گیم یا اپیلی کیشن کو انسٹال کرنے سے پہلے وہ آپ سے آپ کے فیس بک اکاونٹ کے بارے میں پوچھتا ہے۔
تو یاد رکھیں کہ، یہ اپیلی کیشن یا گیم آپ کے فیس بک اکاؤنٹ تک مکمل رسائی بھی حاصل کرسکتا ہے حتیٰ کہ آپ بے شک آف لائن یا لوگ آؤٹ بھی ہو جائیں۔دوسرے لفظوں میں اگر آپ پرمیشن کی ہدایات ٹھیک سے نہیں پڑتے تو آپ اس اپیلی کیشن یا گیم کو اپنے فیس بک معلومات کے علاوہ بھی سب کچھ دے دیتے ہیں، اسلئے کسی گیم، کویز یا اپیلی کیشن کو استعمال کرنے سے پہلے وہ ہدایات پڑھیں اور کوشش کریں کہ صرف مستند گیمز یا اپیلی کیشنز ہی استعمال کریں۔ہم یہ نہیں کہتے کہ سب کمپنیاں ایسی حرکت کرسکتی ہیں، کہ آپ کے اکاونٹ کو غلط استعمال کریں، لیکن بعض ایسا کر بھی سکتی ہیں، اس لئے احتیاط کریں، اور مستند کمپنیوں کے ہی سافٹ ویئرز، یا گیمز استعمال کریں۔

اس خطرے کی ایک مثال آپ کو دیتا ہوں، مثلاً پاکستانی ایجنسی کوئی گیم بناتی ہے فیس بک کیلئے یا اینڈرائیڈ کیلئے اور اسے فیس بک پہ این وائٹ کا کہتی ہے تو جب آپ اسے اپنے فیس بک اکاونٹ کی ایکسس دیتے ہیں تو آرام سے آپ کے تمام میسیجز وغیرہ دیکھ سکتی ہے اگر اس میں پرمیشن مانگی ہے۔
یہ صرف فیس بک نہیں بلکہ ٹوئٹر پہ بھی گیمز، اپیلی کیشن، کوئز وغیرہ بھی آپ کے اکاونٹ پہ پرمیشن مانگتے ہیں۔

لہذا کوشش تو یہی ہو کہ گیمز وغیرہ سے مکمل اجتناب کریں۔

ویڈیو لنک:۔۔۔۔

فیس بک پر ویڈیوز سے بھی محتاط رہیں، کچھ افراد فیس بک پر نامناسب ویڈیوز کے لنک پھیلا رہے ہیں، ,
جس پر کلک کرنے سے غیر موزوں ویڈیوز آپکے فیس بک اکاؤنٹ پر بھی آجائیگی اور کبھی کبھار آپکے فیس بک اکاؤنٹ کا کنڑول حاصل کر کے آپ کے ہی اکاؤنٹ سے وہ لنک دوسروں کی کمنٹس پر مزید شیئر ہو جائیگا، جبکہ آپکو علم بھی نہیں ہو گا کہ میں اس جگہ یہ کمنٹ کیا تھا یا نہیں۔ مثال کے طور پر ایسا بھی دیکھنے میں آیا ہے کہ بعض لوگوں کے اکاونٹس سے بعض دفعہ فحش مواد خود بخود شائع ہونا شروع ہو جاتا ہے، جو کہ ان کے علم میں بھی نہیں ہوتا، اور یوں ان کے دوستوں رشتہ داروں تک اس کے اکاونٹ کی طرف سے جاتا ہے، اور شرمندگی کا باعث بنتا ہے اس لئے محتاط انداز سے فیس بک کا استعمال کریں اور غیر ضروری اور غیر متعلقہ لنکس سے پرہیز کریں۔

اس کی دوسری صورت یہ ہو سکتی ہے کہ کوئی آپ کو فرینڈ بنالیتا ہے اور پھر فحش ویڈیو شئر کرتا ہے اور اس پہ آپ کو ٹیگ کرتا ہے، آپ اس ٹیگ کو ختم کرتے ہیں پھر دوبارہ خود بہ خود آپ اس میں ٹیگ ہوتے ہیں، اگر ایسا کوئی مسئلہ ہو تو آپ فوراً اس بندے کو بلاک کر دیں اور سیٹنگز میں ٹیگ اینڈ ٹائملائن پہ یعنی کون کون آپ کے ٹائم لائن پہ یشئر یا کون آپ کو ٹیگ کر سکتا ہے کے آپشن کو "آنلی می" یعنی صرف میں اس پہ شئر کر سکتا ہوں کے آپشن کو سیلکٹ کریں۔

ڈاؤن لوڈ کا نوٹیفیکیشن:۔۔۔۔۔۔

کبھی کبھار جب آپ کسی ویڈیو کو چلاتے ہیں تو اس ویڈیو کو ڈاؤن لوڈ کرنے کا نوٹیفیکیشن آجائیگا یا کبھی کبھار ویڈیو کو چلانے کیلئے کوڈیک انسٹال کرنے کا نوٹیفیکیشن آجاتا ہے جو ویڈیو چلانے کیلئے لازم ہوتا ہے۔ کبھی کبھار کوڈیک اور فلیش پلیئر کا انسٹال ہونا ضروری ہے، لیکن اس طرح سے اشتہار کی صورت میں آنے والے پیغام اکثر وائرس ہوتے ہیں، جس پر غلطی سے بھی کلک کرنے سے وہ آپکے اکاؤنٹ کے ہیک ہونے کا باعث بن سکتے ہے۔ ایک اچھا اینٹی وائرس ہونے کے باوجود بھی یہ آپکے فیس بک پر اثر کر سکتے ہیں۔ اس لئے ایسی سائٹس اور اس طرح کے پیجز، اکاونٹس اور ویڈیوز سے پرہیز کریں۔ اور اگر کوئی ایسا پلگ اِن انسٹال ہونے کا آپشن آئے تو کبھی بھی انسٹال نہ کرے، اگر فلیش پلئر انسٹال نہیں ہے تو آپ اسے خود انسٹال کریں، یہاں سے انسٹال مت کریں۔

فیس بک انتظامیہ کا میسج:۔۔۔

اگر آپ فیس بک کے کسی پیج کے ایڈمن ہیں، تو یہ بھی ہو سکتا ہے، کہ ہیکر خود کو فیس بک انتظامیہ بتا کر آپکی کوکیز یعنی انٹرنیٹ پر آپ کے دیے گئے معلومات کی وہ فائلیں جو براؤزر کمپیوٹر میں سیو کرتا ہے، ہیکر ان کوکیز کو حاصل کر کے، آپکے پاسورڈ تک رسائی حاصل کر سکتا ہے۔ یہ میسجز بظاہر ایسے ہی لگتے ہیں جیسے فیس بک انتظامیہ ہی کی طرف سے ہو، اور پھر وہ آپکو ایک لنک پر کلک کرنے کا کہتا ہے، جس کے ذریعے وہ آپکی کوکیز چرا لیتے ہیں، اور پھر اس کے ذریعے آپکا فیس بک کا پاسورڈ ہیک کر لیتا ہے۔ اسلئے ایسے میسجز کو نظر انداز کریں۔

خود کو محفوظ بنانے کیلئے مزید ہدایات:۔۔۔۔۔

فیس بک خود بھی سیکیورٹی کو بہتر بنانے کی کوشش کرتا ہے لیکن سماجی رابطوں میں ہونے والی سرگرمیاں انکی پہنچ میں نہیں، اور نہ ہی ایسی غلطیوں کو اینٹی وائرس پکڑ سکتا ہے۔
اگر آپ نے اپنا نمبر فیس بک پر دیا ہے تو اسکی پرائیویسی تبدیل کر کے "آنلی می" یعنی "صرف میں" کر دے جس کے بعد فیس بک پر دیا گیا، آپکا موبائل نمبر صرف آپ ہی دیکھ سکو گے۔ موبائل نمبر دینے کا دوسرا فائدہ یہ ہے کہ اگر آپکا اکاؤنٹ عارضی طور پر بند ہو جائے تو اسے آپ فیس بک کے طرف سے آپکے موبائل پر بھیجے گئے کوڈ کے ذریعے پھر سے چلا سکتے ہیں۔
اکاونٹ عارضی طور پر جو بلاک ہوتا ہے، وہ فیس بک انتظامیہ ہی کی طرف سے ہوتا ہے، تا کہ آپکے اکاؤنٹ کو کسی اور کے ہاتھوں میں جانے سے بچایا جا سکے۔

اسکے لئے ایک دوسرا متبادل طریقہ بھی فیس بک اپناتا ہے اور وہ ہے، "سیکورٹی کے سوالات"۔

اس آپشن میں یہ ہوتا ہے، کہ اکاونٹ عارضی طور پر بند ہونے کے بعد جب آپ لاگ ان ہوتے ہیں، تو یہ آپشن آتا ہے، جس میں فیس بک سیکورٹی میں جاکر اپنی مرضی کے سوالات چن کر انکے جوابات دے سکتے ہیں۔

اگر کوئی آپ کا اکاونٹ ہیک کرنے کی کوشش کرتا ہے، اور فیس بک انتظامیہ کو شک پڑتا ہے، تو فیس بک ایسی صورت میں اکاؤنٹ استعمال کرنے والے سے وہ سیکیورٹی کے سوالات پوچھے گا، اگر وہ درست جوابات دے سکا، تبھی وہ اکاؤنٹ استعمال کر پائیگا، اسلئے ان سوالات کے جوابات کا صرف آپکو پتہ ہونا ضروری ہے اور وہ ہی سوالات چنیں جن کے جوابات آپ یادرکھ سکیں۔

صرف وہ ہی افراد ایڈ کریں جنکو آپ جانتے ہیں۔ کچھ لوگ بغیر جانے بہت سے لوگوں کو اپنے اکاؤنٹ پر فرینڈ بنالیتے ہیں۔ فیس بک انتظامیہ کی طرف سے ایک چیک آسکتا ہے جس میں آپکو یہ بتانا ہوگا کہ مذکورہ تصویر میں کون ہیں، یعنی آپ کے ساتھ جو دوست ایڈ ہیں، یہ تصویر کس دوست نے اپنے اکاونٹ پر لگا رکھی ہے، اس لئے اگر آپ ہر کسی کو ایڈ کرتے رہیں گے، اور آپ اسکو نہیں جانتے ہونگے، اور اس کی پروفائل پر لگی تصویر کو یاد نہیں رکھ پائیں گے، تو فیس بک کو جواب نہیں دے پائینگے، اسلئے ضروری ہے کہ صرف وہی لوگ ایڈ کرے جن کو آپ جانتے ہیں۔

یا اگر آپ مجاہدین کے حوالے سے خبر دیتے اور دیکھتے ہیں اور اکاونٹ فیک ہوتا ہے اور فرینڈ بھی فیک ہوتے ہیں تو آپ کوشش یہ کریں کہ ساتھیوں کے تصاویر دیکھ لیں اور یاد رکھیں۔ اور بہتر یہی ہے کم سے کم اور جو بااعتماد لوگ ہوں ان کو ایڈ کریں۔

لاگ ان نوٹیفیکیشن بھی لگالیں:۔۔۔۔۔۔

اسکے ذریعے آپ جب بھی اپنے فیس بک اکاؤنٹ میں لاگ ان ہوگے، تو آپکے ای میل پر ایک میسج بھیج دیا جائیگا، جسمیں لاگ ان کے معلومات جیسے تاریخ، وقت، آپریٹنگ سسٹم اور براوزر ہوگا۔ اسطرح اگر کوئی اور آپکے فیس بک پر لاگ ان ہوتا ہے تو آپکو اپنی ای میل پر اسکا نوٹی فیکیشن مل جائیگا۔ اسکو آن کرنے کیلئے فیس بک سیکورٹی کے آپشنز والے صفحے پر جائیں۔

اپنے فیس بک اکاؤنٹ کے پاسورڈ کو بار بار یا اکثر بدلا کرے جس طرح آپ اپنے ٹوتھ برش کو بدلتے ہیں ایسے ہی پاسورڈ بھی کچھ مدت کے بعد بدل لیا کریں تاکہ ہیک ہونے سے بچا جاسکے۔

یہ بھی یاد رکھے کہ اپنے ای میل کو خفیہ رکھیں، یعنی فیس بک پر آپکی معلومات میں ای میل پر "آنلی می" کا آپشن ضرور لگالیا کریں۔

۵۔مین-اِن-مڈل/Man-In-Middle

اس کے تفصیل میں ہم نہیں جائینگے بس اتنا سمجھ لیں کہ اس کا حملہ اس وقت ہوتا ہے جب آپ پبلک وائی فائی(یعنی وہ وائی فائی جس میں بہت سے لوگ کنیکٹ ہوں)یا نیٹ کیفے،یا جب بہت سے کمپیوٹر لین /LAN پہ کنیکٹ ہوں،یا انٹرنیٹ کا کنیکشن ایک سے زائد لوگ استعمال کر رہے ہوں،ان جگھوں پہ انٹرنیٹ استعمال کرنے سے یہ حملہ ہو سکتا ہے اور حملہ آور بھی ان میں سے ایک ہوتا ہے جو وہی انٹرنیٹ استعمال کر رہا ہو۔اس میں وہ آپ کے ہر ہر ویبسائٹ کی نگرانی کر سکتا ہے،اپنے فیک فیشینگ ویب سائٹ پر لے جا سکتا ہے اگرچہ آپ کوئی اور ویب سائٹ انٹر کریں پھر بھی وہ اس کو ری ڈائرکٹ کر کہ اپنے فیک ویب سائٹ پر لے جا سکتا ہے،اور وہ یہ بھی کر سکتا ہے کہ آپ جب بھی فیس بک کا سائٹ کھولیں تو وہ آپ کو اپنے فیک فیس بک سائٹ پہ لے جائے اور جب آپ جی میل کا سائٹ کھولیں تو وہ اپنے فیک جی میل سائٹ پہ لے جائے،اس طرح سے وہ آپ کے اکاونٹ ہیک کر سکتا ہے۔اگر کوئی ایکسپرٹ ہو ہیکنگ میں تو وہ آپ کے کمپیوٹر کے ڈیٹا تک رسائی حاصل کر سکتا ہے۔

اس سے بچنے کا کوئی موثر طریقہ نہیں ہے،بس یہ ہے کہ انٹرنیٹ کیفے میں تو کبھی بھی ایسا اکاونٹ نہ کھولیں،اور معلومات شئیر نہ کریں،پبلک وائی فائی میں اگر صرف خاندان کے لوگ ہیں تو کوئی مسئلہ نہیں اگر ویسے عام وائی فائی ہے تو اس سے بھی احتیاط کریں اور ایسے باقی دیگر جگھوں میں دیکھیں جہاں اطمینان ہو اسے استعمال کریں باقیوں کو استعمال نہ کریں۔

۶۔بروٹ فورس/Brute Force

یہ سافٹوئیر میں بھی آتے ہیں اور کوڈنگ سے بھی کرتے ہیں،اس میں ہوتا یہ ہے کہ حملہ آور آپ کا اکاونٹ کھولنے کیلئے ایک لمبی تعداد میں نہ ختم ہونے والی ایک پاسورڈ کی لسٹ آزما لیگا کہ اس میں سے کوئی نہ کوئی لگ جائے۔اس کی دو قسم ہیں:

پہلا طریقہ یہ ہے کہ اس میں سافٹوئیر خود ہی اس پاسورڈ کو ڈھونڈیگا اور aa سے شروع کریگا اس طرح پھر ab پھر ac اور اسی طرح چلتا چلا جائیگا،اور اس میں پاسورڈ ڈھونڈنے میں گھنٹوں لگ جاتے ہیں اور اگر پاسورڈ بہت لمبا ہو اور اس میں #$%^&* اس طرح کے نشانات ہوں تو اس کیلئے تو ایک پورا دن بھی لگ جاتا ہے اور حملہ کرنے والا مایوس ہو کر چھوڑ ہی دیتا ہے۔

دوسرا طریقہ یہ ہے کہ اس سافٹوئیر میں ایک پاسورڈ کی لسٹ ڈالتے ہیں جس میں ۱۰ ہزار سے اوپر پاسورڈ ہوتے ہیں،وہ سافٹوئیر صرف انہی پاسورڈ کو آزمائیگا،یہ پاسورڈ کی لسٹ تو نیٹ پر دستیاب ہیں وہاں سے لوگ لیتے ہیں،مگر چونکہ وہ باہر ممالک کے ہیکرز نے بنائے ہیں اور ہمارے ملک میں لوگ دوسرے پاسورڈ ڈالتے ہیں مثلاً karachi123، maleer12345،وغیرہ،یا کسی کا نام لکھ دیتے ہیں یا کسی کا نمبر لکھ دیتے ہیں اس لئے یہ لسٹ یہاں زیادہ کارآمد نہیں ہوتی البتہ یہاں پھر حملہ کرنے والا اسی مطابق کوئی لسٹ بنائیگا یعنی لوکل لوگ جو پاسورڈ استعمال کرتے ہیں اس حساب سے بناتا ہے۔

بروٹ فورس سے بچنے کیلئے احتیاطی تدابیر:

اپنے پاسورڈ کو لمبا بنائیں،

اس طرح کے نشان ڈالیں ^%&^%()"';'"

اپنے زبان یعنی پشتو، بلوچی، سندھی، پنجابی میں کسی بات کو لے کر پاسورڈ بنائیں، جیسے اردو کی مثال دیتا ہو کہ “$%^&@#kbjaraheho&*^%”

یعنی کوئی ایسا پاسورڈ ہو جو کوئی بھی نہ لیتا ہو، اور علاقے کا نام نہ رکھیں، کسی بندے کا نام نہ رکھیں۔

باقی آپ کوئی سا مشکل پاسورڈ رکھ دیں ان شاءاللہ اس حملہ سے محفوظ رہینگے۔

یہ آخری سبق تھا ہیکنگ کے حوالے سے جس میں بنیادی اور اپنے ڈیٹا اور اکاونٹ محفوظ بنانے سے متعلق ہیکنگ کی معلومات تھیں، باقی ویب سائٹ کی ہیکنگ اس سے علیحدہ ہے چونکہ وہ ہماری ضرورت میں نہیں اس لئے اس کے بارے میں بات نہیں ہوگی جس میں DDOS, SQL injection وغیرہ شامل ہیں۔

اسرار المجاہدین استعمال کرنے کا طریقہ

اسرار المجاین ایک انکرپشن سافٹویر ہے جس کو آپس میں رابطے کیلئے استعمال کرتے ہیں تاکہ جو میسیج بھیج رہے ہیں وہ کسی کو معلوم نہ ہو سکے کہ کیا بھیج رہے ہیں، یعنی آپ میسیج کو کوڈ میں تبدیل کر کہ بھیج دیتے ہیں۔ یہ ضرور استعمال کریں جب آپ مجاہدین سے رابطے کر رہے ہوں، کیوں کہ اس کے بغیر آپ کے میسیج پڑھے جاسکتے ہیں۔

اسرار المجاہدین کو یہاں سے ڈاونلوڈ کریں:

http://pc.cd/c4VctalK

پاسورڈ:

FEjhj*&)(%$jewMoLp^&cioPleWq&*

استعمال کرنے کا طریقہ: اس کا استعمال سیکھنے کیلئے یہ ویڈیو دیکھ لیں، ان شاءاللہ استعمال سمجھ آجائیگی۔

http://ia601007.us.archive.org/4/items/asrar_ur/asrar_ur.avi

نوٹ: کوشش کریں کہ اسرار المجاہدین کو آفلائن ہو کہ استعمال کریں، اور اگر ہو سکے تو یو ایس بی میں ڈال کر ہی استعمال کریں، کمپیوٹر میں نہ ڈالیں۔

امن المجاہد استعمال کرنے کا طریقہ

امن المجاہد، یہ اسرار المجاہدین کی طرح ایک سافٹویر ہے جو میسج انکرپٹ کرنے کا کام کرتی ہے، یعنی یہ ایک انکرپشن سافٹویر ہے جس کے ذریعے میسج بھیجنے والا اور میسج وصول کرنے والے آپس میں پبلک کی/چابی کا تبادلہ کرتے ہیں اور پھر کسی بھی میسج کو انکرپٹ کر سکتے ہیں یعنی اس کو کوڈ میں تبدیل کر کہ وصول کرنے والے پہ بھیج دیا جاتا ہے۔ اس کے علاوہ کوئی فائل انکرپٹ کر کہ بھی بھیجی جاسکتی ہے۔ یہاں آپ کو اینڈرائیڈ ورشن کا بتلا رہے ہیں۔

امن المجاہد کو یہاں سے ڈاونلوڈ کریں:

http://pc.cd/34VctalK

پاسورڈ:

vRkGdU:'{^%HifeE*$@^&$%MnBGdfe

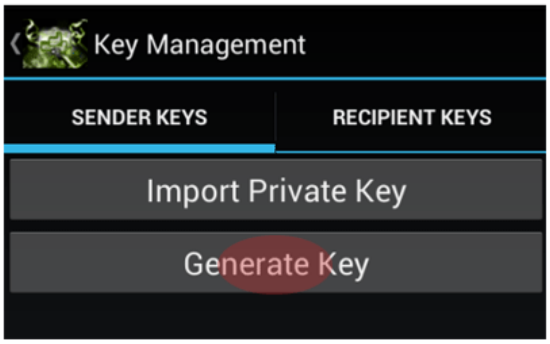
امن المجاہد کے استعمال کا طریقہ:

سب سے پہلے تو اسے ڈاونلوڈ کر کہ انسٹال کریں۔

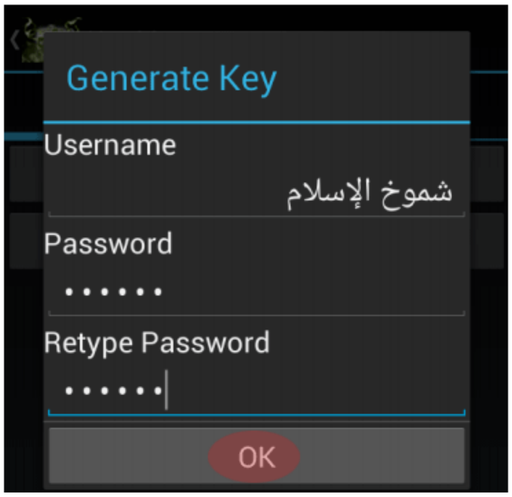
۱۔اپنا 'کی' جنریٹ/پیدا کرنا: سب سے پہلے آپ کو اپنا پرائیویٹ کی اور پبلک کی جنریٹ یعنی پیدا کرنے ہونگے،
اس کیلئے اس ایپ کو کھولیں، پھر اس میں Key Management پہ کلک کریں پھر اس میں Generate Key

1

2



3



4

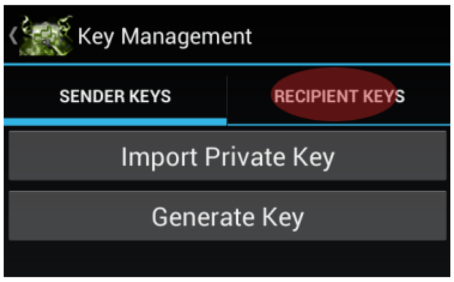
پھر اگلے اسکرین میں username اور پاسورڈ سیٹ کرنے ہونگے، یوزر نیم اور پاسورڈ لکھنے کے بعد ok پہ کلک کریں، دو سے پانچ منٹ لگینگے آپ کا کی جنریٹ ہونے میں۔

پھر جب کی جنریٹ ہو جائیگی تو پھر آپ کا یوزر نیم اسی ٹیب میں ظاہر ہو گا جیسا اوپر تصویر میں دکھایا ہے۔
اور یہ کوئی انٹرنیٹ سافٹوئیر نہیں کہ آپ صرف یہی نام استعمال کریں، بلکہ اس میں آپ ایک وقت میں کئی نام سے کی جنریٹ کر سکتے ہیں۔

۲۔میسج وصول کنندہ سے اُس کا پبلک کی وصول کرنا: یعنی جس کو آپ میسج بھیجنا چاہتے ہیں پہلے اس کا پبلک کی آپ کے پاس ہونا ضروری ہے، تب جا کہ آپ میسج انکرپٹ کر سکینگے۔
پہلے وہ اپنا پبلک کی آپ کو بھیجے گا اور یہ کی اکثر ٹیکسٹ/متن کی صورت میں بھیجتے ہیں۔

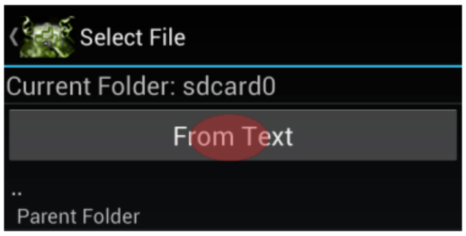
تو اس کی کو یہاں درامد کرنے کیلئے آپ پہلے اس کا مکمل ٹیکسٹ کاپی کریں، پھر اس ایپ میں key management میں Recipient keys پہ کلک کریں۔ پھر اس میں import public key پہ کلک کریں پھر From Text پہ کلک کریں اور اس میں Paste from clipboard کو کلک کریں اگر آپ نے پہلے اس کو کاپی کیا تھا اور پھر اس کی/چابی کا کوئی نام آپ خود رکھ دیں یا اپنے دوست کا نام رکھ دیں۔ پھر ok پہ کلک کریں۔

1

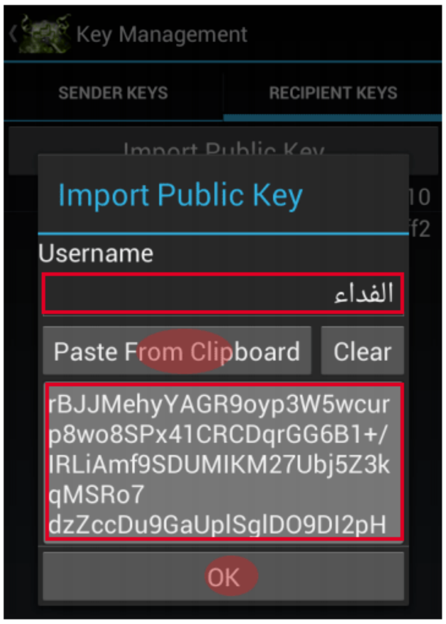


2

3



4

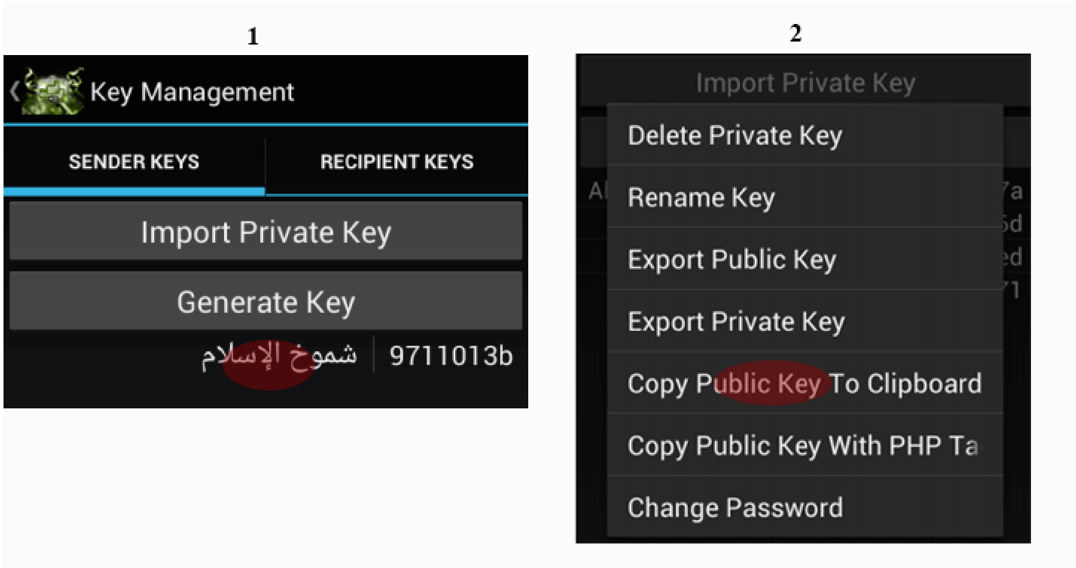


ان تصویروں کو دیکھ لیں، سمجھ آجائیگی۔

پبلک کی یا Recipient Keys میں اب آپ اُس کی کو دیکھ سکتے ہیں جو آپ نے ابھی درآمد / import کی تھی۔

۳۔اپنا پبلک کی برآمد / export کرنا: جس کو آپ انکرپٹڈ میسج بھیجنا چاہتے ہیں، یہ ضروری ہے کہ اُس بندے کے پاس آپ کی پبلک کی موجود ہو، کیونکہ اس کے بغیر میسج ڈی کرپٹ نہیں ہو سکتے یعنی کوڈ سے پھر میسج میں تبدیل نہیں ہو سکتے۔

اپنا پبلک کی ایکسپورٹ کرنے کیلئے Key management میں جائیں، پھر آپ نے جو اپنا کی جنریٹ کیا تھا جس نام سے اس نام پہ کلک کریں، جیسے اس مثال میں شموخ الاسلام کے نام سے جنریٹ کیا تھا، پھر ایک اور ونڈو کھلیگی اس میں Copy Public Key to Clipboard پہ کلک کریں۔



اب آپ کی پبلک کی کاپی ہوگئی ہے اسے اپنے موبائل میں نوٹس میں یا میسج میں یا پھر کسی میں میں پیسٹ کر سکتے ہیں اور جس پہ انکرپٹڈ میسج بھیجنا چاہتے ہیں اس پہ بھیج دیں۔

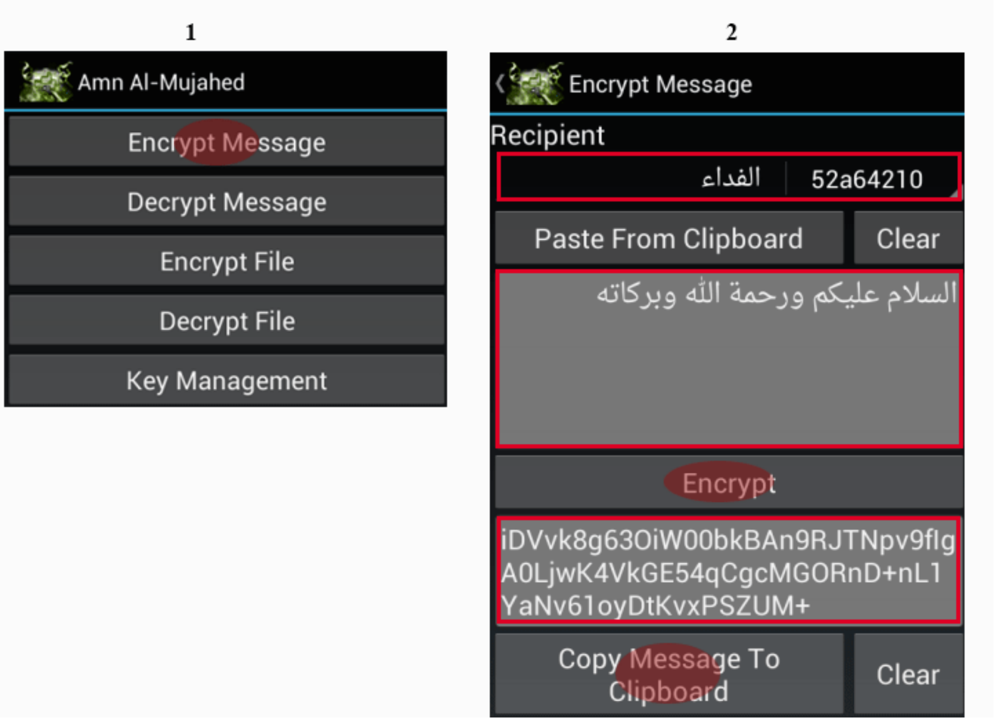
۴۔ میسج کو انکرپٹ کرنا: اپنے میسیج کو انکرپٹ کرنے کیلئے آپ Encrypt Messages پہ کلک کریں،

پھر recipient میں اس بندے کو سیلیکٹ کریں جس کو آپ میسج بھیجنا چاہتے ہیں اور اس کا پبک کی آپ نے درآمد کی ہے، اس مثال میں الفداء کے نام کی پبلک کی درامد کی تھی لہذا اسی کا نام سیلکٹ کرینگے،

پھر نیچے والے خانے میں اپنا میسج لکھینگے، جب میسج پورا ہو جائے تو نیچے Encrypt والے بٹن کو کلک کریں گے،

اب وہ میسج انکرپٹ ہو جائگی، اب اس کو کاپی کرنے کیلئے، copy message to clipboard پہ کلک کریں۔

نیچے تصویر کو دیکھیں سمجھ اجائیگی انشاءاللہ۔



اب آپ کا میسج تیار ہے بھیجنے کیلئے جس کو بھیجنا چاہتے ہیں اس پہ بھیج دیں، اگر ای میل کر رہے ہیں بس پھر ادھر پیسٹ کر دیں اور بھیج دیں۔

۵۔ میسج کو ڈی کرپٹ کرنا: جب آپ کا دوست واپس آپ کو میسج کریگا تو وہ بھی انکرپٹ کر کہ بھیجے گا تو واپس اس انکرپٹڈ کو ڈی کرپٹ کرنے یعنی اس کو ڈوالے میسج کو اصل میسج میں تبدیل کرنے کیلئے آپ اس سافٹویئر میں Decrypt Message پہ کلک کریں،

Recipient میں اس بندے کا پبلک کی کو سیلیکٹ کریں جس کی طرف سے آپ کو میسج آیا ہے،

پھر اگلے خانے میں انکرپٹ شدہ میسج پیسٹ کریں اور پھر Decrypt پہ کلک کریں۔ آپ کا میسج ڈی کرپٹ ہو جائیگا۔

1

2

مائکروسافٹ ورڈ و دیگر فائلز کی معلومات کو ختم کرنے کا طریقہ

جب بھی آپ مائکروسافٹ آفس کی کوئی سافٹویر یا کوئی پی ڈی ایف سافٹویر یا اس جیسے دوسرے سافٹویر استعمال کرتے ہیں تو آپ کی کچھ معلومات اس میں آجاتی ہیں، جس میں کمپیوٹر پہ جو نام رکھا ہے، یا اس سافٹویر میں جو نام لکھا ہے یا اس جیسی دوسرے معلومات اس میں رہ جاتی ہیں، تو ان کو ختم کرنا ضروری ہے اگر آپ اس فائل کو انٹرنیٹ پہ اپ لوڈ کر رہے ہوں۔

مائکروسافٹ ورڈ کا تو ایک مینول یعنی خود سے کرنے کا طریقہ ہے اور دوسرا کسی سافٹویر سے بھی کر سکتے ہیں۔

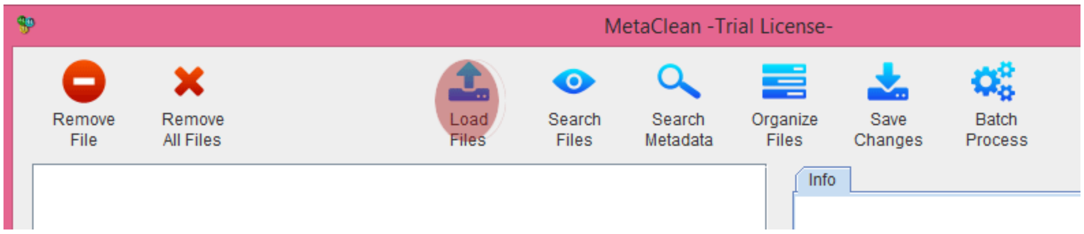
Metaclean سافٹویر سے ان معلومات کو ختم کرنے کا طریقہ: Metaclean سافٹویر تقریباً تمام فارمیٹ کے ساتھ کام کرتا ہے چاہے وہ تصویر ہو یا ویڈیو یا پھر پی ڈی ایف یا ورڈ فائل ہو۔

اس سافٹویر کو یہاں سے ڈاونلوڈ کریں:

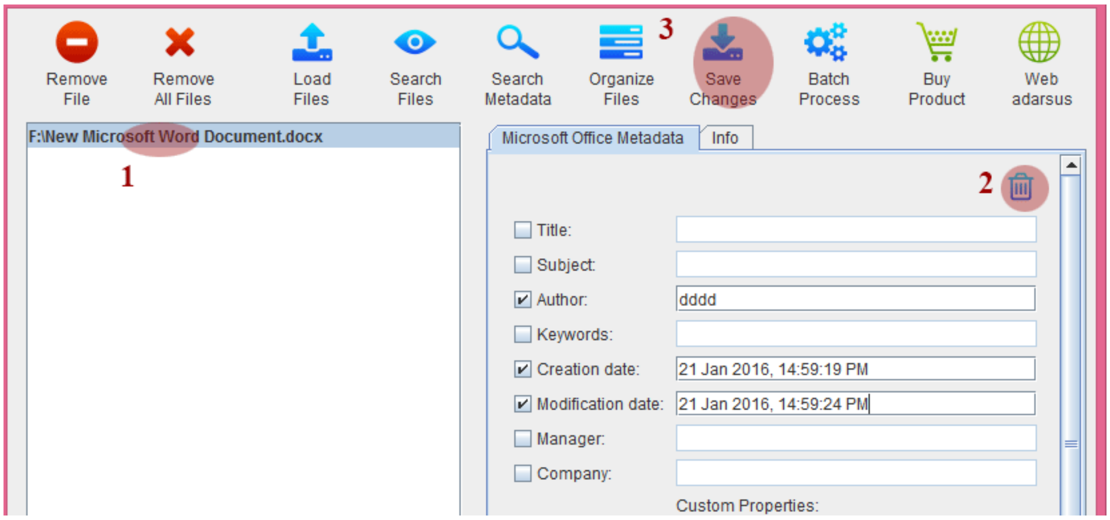
http://www.adarsus.com/en/metaclean.html

نوٹ: یہ فری اور ٹرائل ورژن کا لنک ہے، آپ کو اگر پریمیم ورژن ملے تو وہی ڈاونلوڈ کریں، ٹرائل ورژن میں یہ فرق ہے کہ اس میں بیک وقت ۳ فائل سے زیادہ کو صاف نہیں کر سکتے، باقی معلومات تو ختم ہو جائینگی مگر اس کے ڈیٹیل میں Metaclean سافٹویر کا نام رہے گا، اس کے علاوہ کوئی اور فرق نہیں ہے۔۔۔

ورڈ اور پی ڈی ایف کیلئے استعمال کا طریقہ: انسٹال کر کے کھولیں، پھر اس میں وہ فائل ڈالیں جس کو آپ صاف کرنا چاہتے ہیں، فائل ڈالنے کیلئے آپ Load Files پہ کلک کریں یا پھر ڈارئیکٹ ڈال دیں۔



پھر جو فائل آپ نے ڈالی ہے اسے کلک کریں، دائیں طرف اس کی معلومات لکھی ہونگی۔

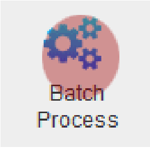


پھر ان معلومات کو سیلیکٹ کریں جن کو ڈیلیٹ کرنا ہے اور پھر ڈیلیٹ والے آپشن کو کلک کریں، جیسا تصویر میں دکھایا ہے،
پھر Save changes پہ کلک کریں، آپ کی فائل سیو ہو جائیگی۔

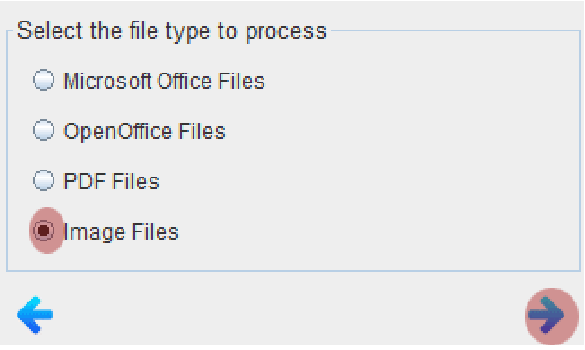
تصویر کیلئے:

فائل ڈالیں، پھر Batch Process پہ کلک کریں، image file پہ کلک کر کہ نیکسٹ کریں،

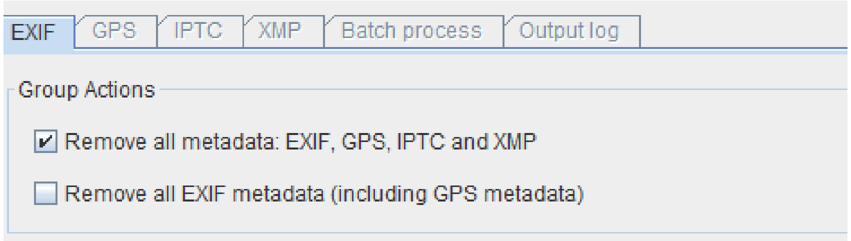
1



2



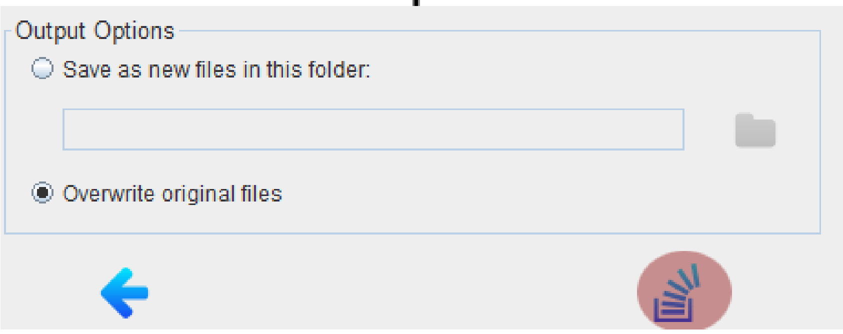
3



پھر اگلے اسکرین میں Remove all metadata:EXIF,GPS,IPTC and XMP پہ کلک کریں

بائیں طرف آخر میں فائل کو سیو کرنے کیلئے اُسی فائل پہ سیلکٹ کریں یا کسی دوسرے نام سے سیو کرنے کا آپشن کلک کریں اور پھر Process پہ کلک کریں، پروسس کا آپشن نیچے تصویر میں دکھایا ہے۔

4



نوٹ: یہ بات یاد رکھیں کہ معلومات اس کی جاتی ہیں جس نے فائل بنایا ہو، یا جس کیمرے یا موبائل سے تصویر لی ہو، مثلاً زید نے کیمرے سے تصویر لی اور بکر کو نیٹ پہ اپ لوڈ کا کہا تو زید کے کیمرے اور موبائل وغیرہ کی معلومات جاسکتی ہیں۔
اسی طرح اگر زید نے کوئی ڈاکومنٹ فائل بنائی اور بکر کو کہا کہ اپ لوڈ کرے تو بکر اگر اسے نیٹ پہ اپ لوڈ کریگا تو زید ہی کی معلومات جائینگی، جب تک کہ بکر اس کو ایڈٹ کر کہ سیو نہ کرے جب وہ ایڈٹ کریگا تو پھر بکر اور زید دونوں کا نام اس میں رہ جائینگی۔

دوسری بات کہ معلومات کس قسم کی ہوتی ہیں؟ مائکروسافٹ ورڈ میں کمپیوٹر لاگ اِن والا نام، یا اگر آپ نے ورڈ پہ دوسرا نام رکھا ہے وہ نام، اس کے علاوہ جو معلومات آپ نے ورڈ میں ڈالی ہیں وہ جائینگی، ویسے اگر دوسری معلومات آپ نہیں ڈالتے یہ دو تو ضرور جاتی ہیں، جس کے بعد ہیکرز کیلئے ہیکنگ کا کام آسان ہوتا ہے۔

پی ڈی ایف میں بھی یہی معلومات جاتی ہیں اس کے علاوہ آپ جس سافٹوئیر سے پی ڈی ایف بناتے ہیں اس کا نام یا اس کے علاوہ بھی اور معلومات

تصویر میں آپ کے موبائل کا نام، کیمرے کا نام، تصویر کی آئی ڈی وغیرہ جاتی ہیں۔ تصویر کا اتنا مسئلہ نہیں کیونکہ ایک قسم کی موبائل کافی لوگ استعمال کر رہے ہوتے ہیں، مگر پھر بھی احتیاط کرنی چاہئے، کیونکہ اگر کوئی آپ کو ٹریس کرنا چاہتا ہے تو اس کے ذریعے سے بھی شک بڑھ سکتا ہے۔

آخری چند باتیں

اب آپ ہیکنگ کے عمل سے واقف ہوگئے ہیں،اب آپ خود بھی کچھ مزید احتیاط کر سکتے ہیں، مثلاًاپنے براوزر کی ہسٹری ڈیلیٹ کریں،اپنے کمپیوٹر کی ہسٹری ڈیلیٹ کریں اور بھی ایسے دیگر ہسٹری وقتاً فوقتاً ڈیلیٹ کریں،اس کے لئے ان دو سافٹوئیر کا استعمال کریں:

Auslogics Boost Speed اور Shellbag analyzer and cleaner

Auslogics کو ٹورنٹ سے ڈاونلوڈ کریں کیونکہ اس کے فری ورشن میں محدود فنکشن ہیں،اور shellbag کیلئے اس لنک پہ کلک کریں،یا انٹرنیٹ سے سرچ کر کہ ڈاونلوڈ کریں۔

http://privazer.com/shellbag_analyzer_cleaner.exe

Auslogics Boost Speed کے کئی فیچرز ہیں، جس میں براوزر کی ہسٹری، ٹیمپرری فائلز، کوکیز، کمپیوٹر کی ہسٹری وغیرہ کو صاف کرنا،
اس کے علاوہ جو فائلز ڈیلیٹ کر چکے ہیں ان کو ہمیشہ کیلئے غائب کرنا تاکہ ری کور نہ ہو سکیں،اس کو ضرور استعمال کیا کریں جو اس کے ٹولز میں
Free Space wiper کے نام سے ہے،اس کے علاوہ اور بھی کئی مفید ٹولز ہیں اس میں۔

باقی Shellbag analyzer and cleaner آپ کے کمپیوٹر کی ہسٹری کو صاف کرتا ہے،اس ہسٹری کو جس کو Auslogics نہیں کر پاتا،یعنی آپ کو یہ دونوں ہی سافٹوئیر استعمال کرنے ہونگے۔

یہ اس لئے استعمال کرنے ہیں تاکہ خدانخواستہ آپ اگر ہیکنگ کا شکار ہو جائیں یا آپ پہ چھاپہ پڑ جائے تو اس صورت میں آپ کے خلاف کوئی ثبوت نہ مل سکے۔۔۔